MEGA ERM

Benutzerhandbuch



MEGA HOPEX V1R1

1. Ausgabe (luglio 2013)

SOMMAIRE

EINLEITUNG

MEGA ERM bietet eine einfache und flexible Lösung für das Management betrieblicher Risiken der Organisation, um die Leistung des Unternehmens nachhaltig zu optimieren.

Das Werkzeug bietet verschiedene Risikomanagementmethoden für die Einhaltung der Vorschriften im Rahmen von Basel II, Solvency II und dem COBIT-Framework an.

Il unterstützt Verantwortliche und Manager im Bereich Risiko, im Risikomanagement eine Methodik einzurichten, die sich an die besonderen Anforderungen eines Unternehmens anpassen lassen.

MEGA ERM Mit dem Tool können alle Schritte im Rahmen des Risikomanagements durchgeführt werden - Definition der Risikoumgebung, Identifizierung, Auswertung und Bearbeitung der Risiken.

PROZESS DES RISIKOMANAGEMENTS

Zusammen mit den Produkten der MEGA-Suite, können Sie die Risiken in **MEGA ERM** identifizieren, bewerten und bearbeiten.

Risiken identifizieren, analysieren und kontextualisieren

Mit einer Risikoanalyse soll das Risiko gut verstanden werden. In der Risikoanalyse müssen die Risikoquellen sowie die positiven und negativen Folgen bzw. Konsequenzen dieses Risikos berücksichtigt werden. Bei einer Analyse werden Ereignistypen, Risikofaktoren (oder Ursachen) Folgen und Ziele mit einem Risiko verbunden.

Mit der Kontextualisierung eines Risikos werden Risiken nach Typ und nach den betroffenen Objekten klassiert. Ein Risiko kann mehrere Typen von Komponenten betreffen: eine *Entität*, einen *Prozess*, eine *Geschäftssparte* oder einen Standort.

Risiken bewerten

Nach der Identifizierung und Analyse der Risiken für ein Unternehmen, wird ihre Bedeutung bewertet, um die wichtigsten Risiken herauszustellen, die bearbeitet werden müssen.

Besonders wichtig ist es, die Ursachen der Risiken zu identifizieren, damit diese Risiken, und nicht nur ihre Symptome bearbeitet werden. Die Risiken werden auf Grundlage ihrer Häufigkeit, ihrer Auswirkung, Kontrollstufe und Effizienz bewertet. Diese Bewertung dient als Grundlage zur Bestimmung der Art und Weise, wie die Risiken gemanagt werden.

Um die Risikoanalyse nach der Bewertung einfacher zu gestalten, werden Standardberichte geliefert:

- "Die Aggregationen", Seite 87
- "Effizienz des Risikomanagements", Seite 95
- "Trendanalyse", Seite 96

Für die Bewertung gibt es zwei Möglichkeiten:

- die direkte Bewertung, mit der ein Experte die globale Bewertung eines Risikos zu einem bestimmten Datum aufstellen kann.
- die Bewertung nach Kampagnen, mit der Risiken und Kontrollen nach Entitäten und nach Prozessen ab Standardfragebögen bewertet werden können.

Risiken bearbeiten

Risiken zu bearbeiten beinhaltet, verschiedene mögliche Optionen zu identifizieren, diese Optionen zu beurteilen und Pläne zur Bearbeitung bzw. Reaktion vorzubereiten und umzusetzen.

Der Konzeption von Aktionen zur Risikobearbeitung liegt eine fundierte Kenntnis der betroffenen Risiken zu Grunde; diese Kenntnis oder dieses Verständnis ist darauf zurückzuführen, dass die Risikoanalyse auf einer angemessenen Ebene durchgeführt wird. .

Allgemein ist es nicht rentabel oder sogar wünschenswert, alle möglichen Bearbeitungen des Risikos durchzuführen. Es ist jedoch notwendig, eine Kombination der Risikobearbeitungen zu wählen und umzusetzen, die sich am besten eignet.

Die Bewertung von Risiken ist also ein wichtiger Schritt, um eine Liste von Risiken zu erhalten, die eventuell - mit gewissen Prioritäten - bearbeitet werden müssen.

DIE BENUTZERROLLEN

In **MEGA ERM**, sind standardmäßig Benutzerrollen enthalten, denen Zugriffsrechte zugewiesen werden. Verfügbare Rollen:

- Funktionaler Risikoadministrator
- Risk Manager und lokaler Risk Manager
- Branchenspezifischer Benutzer der Lösung
- Risikobewerter
- Risiko-Interessensgruppe

Funktionaler Risikoadministrator

Der funktionale Administrator hat Rechte für alle Objekte und Workflows.

Er bereitet die Arbeitsumgebung vor und erstellt die für das Risikomanagement notwendigen Elemente.

Er verwaltet:

- die Beschreibung der Umgebung
  - organisatorische Einheiten und Prozesse
  - die Umgebung der Vorschriften
  - die IT-Ressourcen

    ☛ *Weitere Informationen zur Beschreibung der Umgebung finden Sie im Handbuch **HOPEX Solutions Common Features**.*
- die Benutzer und Zuweisung der Rollen

Er kann einwirken auf:

- die ermittelten Risiken
- die Bewertungskampagnen
- die Aktionspläne und Aktionen

Risikomanager

Um sich an ein zentrales oder dezentrales Risikomanagement anzupassen, unterscheidet **MEGA ERM** zwischen einem **Risikomanager** und **lokalen Risikomanagern**.

Der Risk Manager ist für die Ausführung folgender Aufgaben im Zusammenhang mit den Risiken in seinem Verantwortungsbereich zuständig:

- Risikoidentifizierung
- Direkte Bewertung
- Management von Bewertungskampagnen
- Definition von Aktionsplänen
- Erstellen und Aktualisierung von Analyseberichten und Berichten von Folgemaßnahmen

Branchenspezifischer Benutzer der Lösung

Der Endbenutzer der Lösung ist für die Identifizierung und Charakterisierung der Risiken und Kontrollen in seinem Wirkungskreis zuständig. Er kann die Umsetzung der Aktionspläne für diese Risiken vorschlagen.

Der branchenspezifische Benutzer ist für folgende Aufgaben zuständig:

- Risikoidentifizierung
- Beantwortung der Fragen der Fragebögen
- Festlegung und Umsetzung der Aktionspläne
- Aufrufen und Erstellen von Berichten

Risikobewerter

Der Risikoexperte ist für die Bewertung der Risiken in seinem Wirkungskreis zuständig. Er ist ebenfalls für die Umsetzung der Aktionspläne für diese Risiken zuständig. Er ist für folgende Aufgaben verantwortlich:

- Beantwortung der Fragen der Fragebögen
- Ausführung der Aktionen eines Aktionsplans

Risiko-Interessensgruppe

Eine Interessengruppe bei einem Risiko ist ein Zusammenschluss von Personen bzw. hier eine Person, die von einem Risiko betroffen ist, wenn es eintritt. Dabei beschränkt sich die Interessengruppe in ihrer Funktion darauf, Berichte der Unternehmensführung einzusehen, die vom Risikomanager erstellt wurden, und ihn im Fall eines nicht identifizierten oder eines bestätigten Risikos zu warnen.

ÜBER DIESES HANDBUCH

n diesem Handbuch wird erklärt, wie Sie mit **MEGA ERM** für ein effizientes Risikomanagement sorgen können.

Struktur des Handbuchs

Das Handbuch **MEGA ERM** setzt sich aus folgenden Kapiteln zusammen:

- "Der Arbeitsbereich", Seite 15, beschreibt die Schritte vor der Nutzung dieser Lösung und stellt die Benutzeroberfläche abhängig vom verbundenen Benutzer vor.
- "Funktionale Administration", Seite 25, beschreibt die Initialisierungen der Referenzdaten, die implementiert werden müssen, bevor mit dem Risikomanagement begonnen wird.
- "Risiken verwalten", Seite 29, präsentiert die Funktionalitäten in **MEGA ERM**, um die Risiken zu charakterisieren.
- "Überwachung der Kontrollpolitik", Seite 41, präsentiert die Funktionalitäten in **MEGA ERM**, um die Kontrollen zu charakterisieren.
- "Bewertungen mit MEGA ERM", Seite 47, erklärt, wie die verschiedenen Tools zur Risikobewertung funktionieren, die in **MEGA ERM** enthalten sind.
- "Risiken bearbeiten", Seite 69, erklärt, wie Aktionspläne funktionieren.
- "Die Berichte MEGA ERM", Seite 81, präsentiert die Berichte in **MEGA ERM** für die Analyse der Risiken.
- "Glossar", Seite 97, fasst die Definitionen der wichtigsten Konzepte zusammen, die im Handbuch **MEGA ERM** erwähnt werden.
- "Anhang - Workflow von MEGA ERM", Seite 103, beschreibt die Workflows, die standardmäßig in **MEGA ERM** enthalten sind.

Dieses Handbuch wird ergänzt durch:

- **das Handbuch HOPEX Solutions Common Features**, in dem die spezifische Web-Benutzeroberfläche der MEGA-Lösungen beschrieben wird.

  ☛ *Es kann nützlich sein, dieses Handbuch aufzurufen, um eine allgemeine Darstellung der Benutzeroberfläche zu erhalten.*

- das Administrationshandbuch **MEGA Administration - Supervisor**.

Weitere Ressourcen

Dieses Handbuch wird ergänzt durch:

- **das Handbuch HOPEX Solutions Common Features**, in dem die Web-Benutzeroberfläche und die spezifischen Tools der MEGA-Lösungen beschrieben werden.

  ☛ *Es kann nützlich sein, dieses Handbuch aufzurufen, um eine allgemeine Darstellung der Benutzeroberfläche zu erhalten.*

- das Administrationshandbuch **MEGA Administration - Supervisor**.

Schreibkonventionen in diesem Handbuch

Stil und Formatierung

☛ *Anmerkung zu den vorherigen Punkten.*

📖 *Definition der verwendeten Begriffe.*

☺ *Tipp, der dem Benutzer das Leben erleichtern kann.*

Kompatibilität mit vorherigen Versionen.

Zu vermeiden.



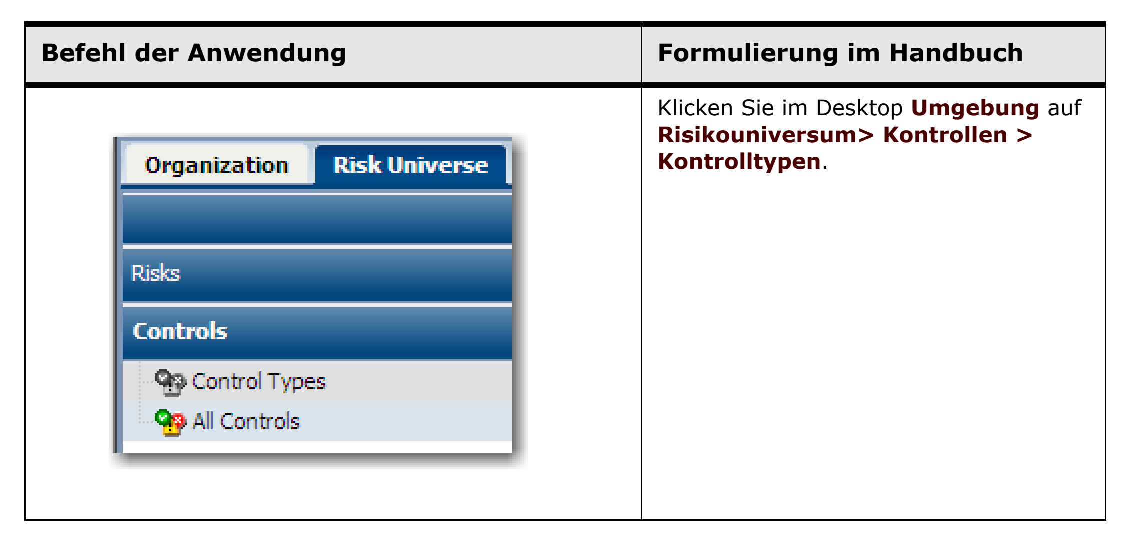
Wichtiger Hinweis zur Vermeidung von Bedienungsfehlern.

Befehle werden wie folgt dargestellt: **Datei > Öffnen**.

Namen von Produkten und technischen Modulen werden wie folgt dargestellt: **MEGA**.

Formulierung einer Befehlsfolge

Um eine Befehlsfolge zu beschreiben wird in diesem Handbuch der Einfachheit halber folgende Formulierung verwendet:



Befehl der Anwendung	Formulierung im Handbuch
	Klicken Sie im Desktop **Umgebung** auf **Risikouniversum> Kontrollen > Kontrolltypen**.

Beispiel eines Befehls mit Formulierung im Handbuch

Der Arbeitsbereich

Dieses Kapitel macht Sie mit der Verwendung von **MEGA ERM** vertraut und stellt die einzelnen Schritte vor, die vor der Nutzung der Lösung durchzuführen sind.

☛ *Ausführliche Informationen zu den Funktionalitäten von **MEGA**finden Sie in den Handbüchern **MEGA Common Features** und **HOPEX Solutions Common Features**, in denen die Funktionalitäten erklärt werden, die von allen Produkten der **MEGA**-Suite angeboten werden.*

Hier werden die folgenden Punkte erörtert:

Grundvoraussetzungen für die Verwendung von MEGA ERM

Um **MEGA ERM** zu verwenden, muss der Administrator zuvor einige Schritte durchführen.

Spezifische Bibliotheken importieren

MEGA ist installiert.

Um auf die **MEGA ERM**-spezifischen Funktionen zuzugreifen, die in diesem Handbuch beschrieben werden, müssen Sie sicherstellen, dass der Administrator folgende Prozeduren durchgeführt hat.

Importe vorbereiten

Die zu importierenden Dateien werden als komprimierte Dateien mitgeliefert, die dekomprimiert werden müssen, bevor sie in ein Repository importiert werden.

Um die **MEGA ERM**-spezifischen Dateien zu dekomprimieren, gehen Sie wie folgt vor:

1. Öffnen Sie im Ordner, in dem **MEGA** installiert wurde, den Ordner **Dienstprogramme** und anschließend den Ordner **MEGA FrameWork**.
2. Doppelklicken Sie auf die Datei **ERM.exe**.
3. Klicken Sie in dem nun geöffneten Dialogfenster auf **Installieren**.
   Es werden zwei neue Verzeichnisse erstellt: **ERM - Sample** und **ERM - Technical**.

Dateien zur Nutzung von MEGA ERM importieren

Um **MEGA ERM** -Spezifische Objekte zu importieren, gehen Sie wie folgt vor:

1. Starten Sie "Administration.exe" und verbinden Sie sich mit einem Benutzer, der über die Administrationsberechtigung für Daten verfügt.

   ☛ *Mit der ID "System" können Sie sich mit "Administrator" als Benutzer verbinden. Dieser Benutzer wird standardmäßig mit den Rechten zur Administration der Repositorys erstellt. Er besitzt weder Profil (er hatte alle Berechtigungen) noch ein Kennwort, das ihm bei der Installation zugewiesen wurde.*
2. Wählen Sie die Umgebung und anschließend das Repository aus, mit dem Sie arbeiten möchten.
3. Klicken Sie mit der rechten Maustaste auf das Repository und wählen Sie **Verwaltung der Objekte > Solution Pack importieren** aus.
   Dann wird das Fenster zur Auswahl des Solution Packs angezeigt.
4. Wählen Sie **ERM - Technical** aus und klicken Sie auf **OK**.
   Sie haben ein leeres Repository erstellt.
5. Beenden Sie die Anwendung Administration.

Beispielbibliothek importieren

Wenn Sie ein Repository mit einem Beispiel verwenden möchten, gehen Sie wie folgt vor:

1. Starten Sie "Administration.exe" und verbinden Sie sich mit einem Benutzer, der über die Administrationsberechtigung für Daten verfügt:
2. Wählen Sie die Umgebung und anschließend das Repository aus, mit dem Sie arbeiten möchten.
3. Klicken Sie mit der rechten Maustaste auf das Repository und wählen Sie **Verwaltung der Objekte > Solution Pack importieren** aus.
   Dann wird das Fenster zur Auswahl des Solution Packs angezeigt.
4. Wählen Sie **ERM - Sample** aus und klicken Sie auf **OK**.
5. Beenden Sie die Anwendung Administration.

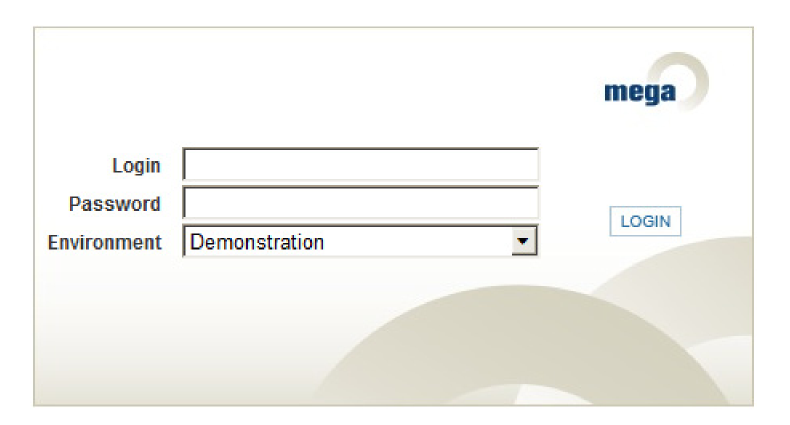
VERBINDUNG ZU MEGA ERM

Um sich mit einer **MEGA** -Anwendung im Web zu verbinden, gehen Sie wie folgt vor:

1. Starten Sie die Anwendung **MEGA** unter ihrer HTTP-Adresse.

   ☛ *Wenn Sie die Adresse nicht kennen, wenden Sie sich an Ihren Administrator.*

   Daraufhin wird die Verbindungsseite geöffnet.



2. Geben Sie auf der Verbindungsseite im Feld **Login** Ihre ID ein.
3. (Wenn Sie ein Kennwort besitzen) Geben Sie im Feld **Password** Ihr Kennwort ein.

   ☛ *Wenn Sie Ihr Kennwort vergessen haben, klicken Sie auf* Lost password *(unter dem Verbindungsfenster).*

4. Klicken Sie im Feld **Environment** auf den Pfeil und wählen Sie die Arbeitsumgebung aus.

   ☛ *Sollten Sie keinen Zugriff auf eine Umgebung haben, wird die Umgebung automatisch berücksichtigt. Das Feld zur Auswahl der Umgebung wird nicht angezeigt.*

5. Klicken Sie auf **LOGIN**.
   Wenn Sie authentifiziert wurden, wird ein neues Fenster angezeigt.
6. Klicken Sie im Feld **Repository** auf den Pfeil und wählen Sie das Arbeits-Repository aus.

   ☛ *Sollten Sie nur auf ein Repository Zugriff haben, wird das Repository automatisch berücksichtigt. Das Feld zur Auswahl des Repositorys wird nicht angezeigt.*

7. Klicken Sie im Feld **Profile** oder **Role** auf den Pfeil und wählen Sie das Profil oder die Rolle aus, mit der bzw. dem Sie arbeiten möchten.

   ☛ *Sollten Sie keinen Zugriff auf ein Profil oder eine Rolle haben, wird das Profil oder die Rolle automatisch berücksichtigt. Das Feld zur Auswahl des Profils oder der Rolle wird nicht angezeigt.*

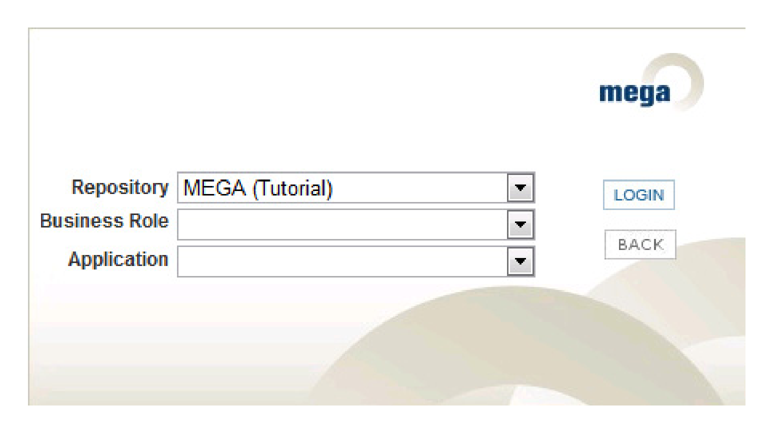
   ☛ *In **MEGA Administration** wird das Feld **Role** statt **Profile** angezeigt, wenn in den Optionen der Umgebung (Optionen/Installation/*

Benutzerverwaltung) die Option "Verwaltung der Zuweisung von Geschäftsrollen an Personen" ausgewählt wurde.

☛ *Das ausgewählte Profil bzw. die Rolle definiert die Anwendungen, auf die Sie zugreifen können.*

8. Klicken Sie im Feld **Application** auf den Pfeil und wählen Sie die Anwendung aus, mit der Sie sich verbinden möchten.

☛ *Sollten Sie keinen Zugriff auf eine Anwendung mit dem ausgewählten Profil bzw. der Rolle haben, wird das Profil/die Rolle automatisch berücksichtigt. Das Feld zur Auswahl der Anwendung wird nicht angezeigt.*



9. Klicken Sie auf **LOGIN**.

☛ *Klicken Sie auf **BACK**, wenn Sie zum Authentifizierungsfenster zurückkehren möchten.*

Die Home-Page der Web-Anwendung wird angezeigt und eine Sitzung wird geöffnet.

☛ *Weitere Informationen zur Definition der Benutzer und Rollen finden Sie im **Handbuch für den Administrator**, Kapitel "Benutzer verwalten".*

Präsentation der Benutzeroberfläche

Die Menüs und Befehle in **MEGA ERM** hängen von der Geschäftsrolle ab, mit der Sie verbunden sind.

> ☛ *Weitere Informationen zu den Geschäftsrollen finden Sie unter "Die Benutzerrollen", Seite 12.*

> ☛ *Weitere Informationen zur Verwendung der Web-Plattform im Rahmen der HOPEX-Lösungen finden Sie im Handbuch **Hopex Solutions Common Features**.*

Bereich für den funktionalen Administrator der Risiken

Der funktionale Administrator verfügt über drei Desktops:

- den Desktop **Administration**
- den Desktop **Umgebung**, in dem die Arbeitsumgebung definiert wird Siehe "Arbeitsumgebung vorbereiten", Seite 26.
- den Desktop **ERM** , mit sechs Registerkarten, die den wichtigsten Schritten im Rahmen des Risikomanagements entsprechen:
  - **Home**: für einen einfacheren Zugriff auf die verschiedenen Ordner und Objekte, für die der Benutzer verantwortlich ist
  - **Risikobibliothek**: für den Zugriff auf die Liste der Risiken und Kontrollen. Ab dieser Registerkarte können direkte Bewertungen durchgeführt werden.
  - **Kampagnenmanagement**: Registerkarte für die Verwaltung der Risikobewertung anhand von Kampagnen.
  - **Bearbeitung**: um Aktionspläne und Kontrollen für die Bearbeitung der Risiken anzugeben und durchzuführen.
  - **Berichte**: für den Zugriff auf alle Berichte, mit denen Kontrollen und Risiken analysiert und nachverfolgt werden können.
  - **Dokumentbibliothek**: Registerkarte für den Zugriff auf die Dokumente, die mit dem Risikomanagement verbunden sind.

Bereich für den Risk Manager

Dem Risk Manager stehen zwei Desktops zur Verfügung: **Umgebung** und **ERM** , die identisch zu den Desktops des funktionalen Administrators der Risiken sind.

Bereich für den Risikobewerter

Neben der Registerkarte **Home** stehen dem Risikobewerter zwei Registerkarten zur Verfügung: **Risikobibliothek** und **Kampagnenmanagement**.

Bereich für den Geschäftsbenutzer der Lösung

Der Geschäftsbenutzer verfügt ebenfalls über die zwei Registerkarten: **Risikobibliothek** und **Kampagnenmanagement**.

Bereich für den Benutzer Risiko-Interessensgruppe

Dieser Benutzer verfügt lediglich über die Registerkarte **Home**, in der die Objekte aufgeführt werden, für die er zuständig ist.

FUNKTIONALE ADMINISTRATION

Damit die verschiedenen Teilnehmer ihre Geschäftsrollen erfüllen können, muss der funktionale Administrator zuvor die Arbeitsumgebung vorbereiten.

Es handelt sich um folgende Aufgaben:

- ✓ "Organisation definieren", Seite 26
- ✓ "Umgebung der Vorschriften beschreiben", Seite 26
- ✓ "Ressourcen des Unternehmens beschreiben", Seite 28
- ✓ "Risiken beschreiben", Seite 28
- ✓ "Kontrollen beschreiben", Seite 28

Arbeitsumgebung vorbereiten

Folgende Punkte erklären, wie die Elemente erstellt werden, die Ihre Arbeitsumgebung bilden. Dieser Schritt muss vom funktionalen Administrator durchgeführt werden.

☛ *Weitere Informationen zu den Komponenten der funktionalen Umgebung finden Sie im Handbuch* ***HOPEX Solutions Common Features.***

Organisation definieren

Die Organisation eines Unternehmens ist in große Komponenten unterteilt: *Prozesse*, *Entitäten* und *Geschäftssparten*:

Ein Prozess ist eine Wertekette, die einem internen oder externen Kunden Güter oder Services bereitstellt. Diese Wertekette wird durch eine Folge von Aktivitätsumwandlungen beschrieben. Sie wird von den Abläufen implementiert.

Eine Entität kann unternehmensintern oder -extern sein: Eine Entität stellt ein Element der Struktur eines Unternehmens dar, wie beispielsweise eine Direktion, eine Abteilung oder einen Arbeitsplatz. Sie wird auf einer mehr oder weniger genauen Ebene definiert, je nachdem, wie präzise die Angaben über die Organisation sein müssen (siehe Organisationseinheitstyp). Beispiel: Finanzdirektion, Vertrieb, Marketingabteilung, Vertriebsmitarbeiter. Eine externe Entität stellt eine Einrichtung dar, die Flüsse mit dem Unternehmen austauscht. Beispiel: Kunde, Lieferant, Administration.

Eine Geschäftssparte ist eine hohe Klassierungsebene der wichtigsten Geschäftstätigkeiten eines Unternehmens. Sie entspricht zum Beispiel großen Produktsegmenten oder Distributionskanälen. Sie ermöglicht, Prozesse eines Unternehmens, organisatorische Einheiten oder Anwendungen für ein bestimmtes Produkt und/oder einen bestimmten Markt zu klassieren. Regelwerke bestimmter Industrien schreiben ihre eigene Liste von Geschäftssparten vor.

Diese Komponenten werden in Form einer Baumstruktur aufgeführt.

Für den Zugriff gehen Sie wie folgt vor:

- Wählen Sie **Umgebung > Organisation > Hierarchische Ansichten** aus.

Umgebung der Vorschriften beschreiben

Die Vorschriften

Die zu berücksichtigenden *Vorschriften* können finanzieller (SOX, LSF, usw.) und sektorieller (Basel II, Solvency II, Seveso II, usw.) Art sein, sich auf den Personenschutz beziehen usw.

Eine Vorschrift oder eine interne Regelung stellt mehrere Richtlinien mit oder ohne Bedingungen auf, die von der Regierung im Rahmen

eines Gesetzes, von einem Berufsverband in Form von Best Practices oder intern von einer Organisation festgelegt werden.

Für den Zugriff auf die Liste der *Vorschriften* gehen Sie wie folgt vor:

- Wählen Sie **Umgebung > Umgebung der Vorschriften > Vorschriften** aus.

Die Anforderungen

Um sicherzustellen, dass Ihre Organisation die strategischen Erwartungen des Unternehmens erfüllen, können die wichtigsten **MEGA** -Konzepte mit *Anforderungen* verbunden werden.

> *Eine Anforderung ist ein explizit ausgedrückter Bedarf oder eine Erwartung, die wie eine Einschränkung vorgeschrieben und im Rahmen eines Zertifikations-, Organisations- oder Modifikationsprojekts für das Informationssystem des Unternehmens erfüllt werden muss.*

Um auf die Baumstruktur der *Anforderungen* zuzugreifen, gehen Sie wie folgt vor:

- Wählen Sie **Umgebung > Umgebung der Vorschriften > Anforderungen** aus.
  Daraufhin werden die Anforderungen der Organisation hierarchisch angezeigt.

Die Ziele

> *Ein Ziel ist ein Ergebnis, das erreicht werden soll, oder das angestrebte Resultat eines Prozesses oder eines Arbeitsschritts. Mit einem Ziel können die Punkte hervorgehoben werden, die für diesen Prozess oder diesen Arbeitsschritt verbessert werden sollen.*

Ein *Ziel* kann quantitativ, das heißt direkt messbar, oder qualitativ sein.

- Die Frist zwischen Bestellung und Lieferung verkürzen (quantitatives Ziel)
- Die Qualität des Produkts verbessern (qualitatives Ziel)
- Die Kundenzufriedenheit erhöhen (qualitatives Ziel)

Um auf die Baumstruktur der *Ziele* zuzugreifen, gehen Sie wie folgt vor:

- Wählen Sie **Umgebung > Umgebung der Vorschriften > Ziele** aus.
  Daraufhin werden die Ziele der Organisation hierarchisch angezeigt.

  Wenn Sie den Ordner eines Ziels aufklappen, kann die Baumstruktur der Unterziele eines aktuellen Ziels angezeigt werden.

> *Die Liste der Ziele im Besitz eines Ziels kann in der Eigenschaftsseite des Ziels, in der Registerkarte **Merkmale**, im Abschnitt **Unterziele** geöffnet werden.*

Ressourcen des Unternehmens beschreiben

Die Beschreibung eines Kontextes, in dem ein Risikomanagementprojekt abgewickelt wird, kann auch mit der Beschreibung von IT-*Anwendungen*, Datenbanken und *Servern* als Host ergänzt werden.

Eine Anwendung besteht aus Software-Komponenten, die im Rahmen der IT-Entwicklungen eine konsistente Einheit bilden.

Eine Datenbank ermöglicht, die logische oder physische Speicherungsstruktur der Daten anzugeben.

Ein Server ist eine Hardware-Ressource, die über eine Datenbank verfügen kann, auf der eine Anwendung ausgeführt werden kann.

Für den Zugriff auf die Liste der IT-Ressourcen gehen Sie wie folgt vor:

- Wählen Sie **Umgebung > Ressourcen** aus.

Risiken beschreiben

Der funktionale Administrator besitzt die Rechte, alle Informationen zu aktualisieren, mit denen die Risiken und Kontrollen charakterisiert werden können.

☛ *Weitere Informationen zur Verwendung erwarteter Informationen für die Risikoanalyse finden Sie unter "Risiken identifizieren", Seite 31.*

Kontrollen beschreiben

Der funktionale Administrator besitzt die Rechte, Informationen zu aktualisieren, mit denen die Kontrollen charakterisiert werden können.

☛ *Weitere Informationen zur Verwendung von Informationen für die Risikoanalyse finden Sie unter "Kontrollen verwalten", Seite 42.*

RISIKEN VERWALTEN

Um die *Risiken* unter Kontrolle zu halten, müssen die Risiken im Ablauf eines Prozesses erkannt und eingestuft werden.

Ein Risiko ist eine mehr oder weniger wahrscheinliche Gefahr, der einer Organisation ausgesetzt ist.

Wenn die Risiken analysiert und bewertet sind, legt das Management die Bearbeitungen fest, die für die jeweiligen Risiken in Frage kommen. **MEGA ERM** bietet Werkzeuge, mit denen die Risiken einfacher erstellt und analysiert werden können, um dann die wichtigsten Risiken zu identifizieren und geeignete korrektive oder präventive Maßnahmen zu treffen.

Hier werden die folgenden Punkte erörtert:

☛ *Weitere Informationen zur Verwendung der Analyseberichte über Risiken finden Sie unter* *"Die Berichte MEGA ERM", Seite 81.*

EINFACHER ZUGRIFF AUF DIE AUFGABEN

Sie können auf die verschiedenen Ordner und Objekte, für die Sie verantwortlich sind, einfach zugreifen, wenn Sie auf **Risiko > Home > Mein Desktop** klicken. Im Desktop können Sie zugreifen auf:

- Ihre Verantwortungsbereiche
  - Bewertungsfragebögen
  - Risiken
  - Kontrollen
  - Aktionspläne
  - Kampagnen
- Ihren Umfang
  - Risiken
  - Kontrollen
  - Aktionspläne
- Ihre Benachrichtigungen
  - nicht gelesene Benachrichtigungen
  - gelesene Benachrichtigungen

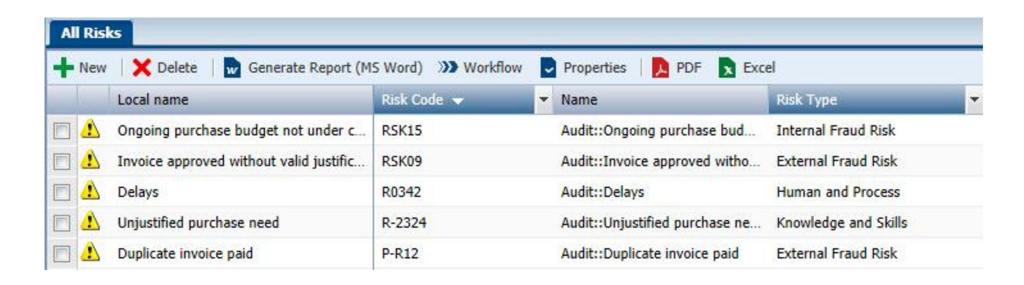
RISIKEN IDENTIFIZIEREN

Auf die Liste der Risiken zugreifen

Die Liste der Risiken kann mit dem Befehl **Risiko** > **Risikobibliothek > Risiken** geöffnet werden.

Im Ordner **Risiken** können Sie auf die verschiedenen Listen der Risiken zugreifen:

- Alle Risiken
- Hauptrisiken, d. h. die höchsten Risiken
- Risiken ohne Kontrolle



Eigenschaften eines Risikos

Um auf die Merkmale eines Risikos zuzugreifen, gehen Sie wie folgt vor:

- Wählen Sie in einer Liste der Risiken ein Risiko aus und klicken Sie auf die Schaltfläche **Eigenschaften**.
  Das Eigenschaftsfenster des Risikos wird in der Bearbeitungszone angezeigt.

Im Abschnitt **Merkmale** können Sie angeben:

- den **Identifizierungscode** des Risikos
- den **Namen** des Risikos
- die hohe Risikostufe, wenn Sie das Kästchen **Hauptrisiko** markieren
- den **Eigentümer** des Risikos
- den **Identifizierungsmodus** des Risikos
  Das Risiko kann identifiziert werden durch:
  - "Fragebögen"
  - ein "Ereignis-Repository"
  - einen "Workshop"
  - eine "Expertise" (durch einen unternehmensinternen oder -externen Experten)
  - einen "Workshop"
  - eine "Stichprobe",
  - ein "Audit"
- die **Beschreibung** des Risikos

☛ *Der **Status des Risikos** wird abgeblendet angezeigt, weil er vom Workflow des Risikos verwaltet wird. Weitere Informationen finden Sie unter* *"Prozess der Erstellung eines Risikos", Seite 35**.*

Der Umfang eines Risikos

Mit dem Umfang eines Risikos kann die Lokalisierung eines Risikos im Unternehmen bestimmt werden.

☛ *Die Organisation wird ausführlich im Handbuch **HOPEX SolutionsCommon Features** beschrieben.*

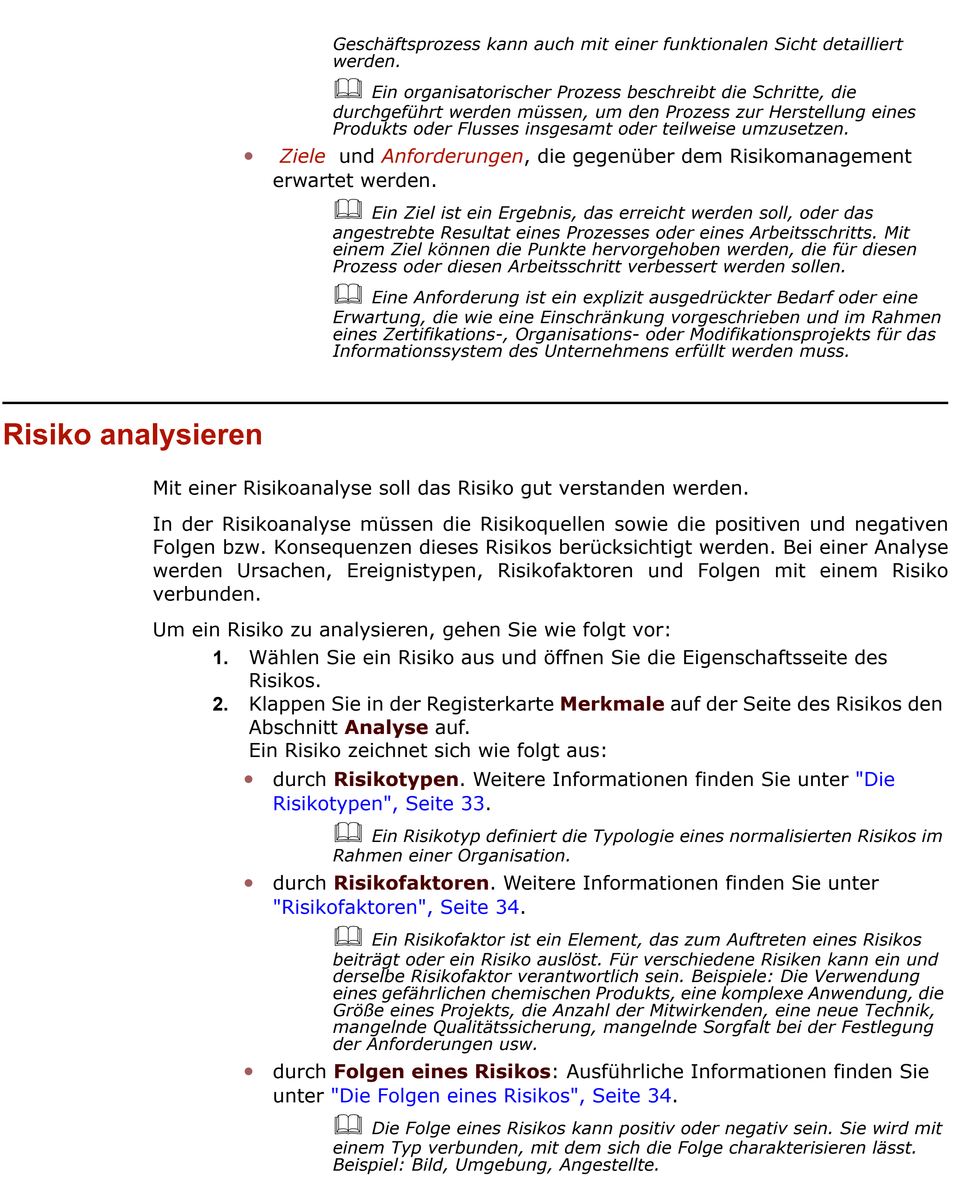
Der Umfang wird bei mehreren Komponententypen angegeben:

- *Entitäten*, die vom Risiko betroffen sind.

  Eine Entität kann unternehmensintern oder -extern sein: Eine Entität stellt ein Element der Struktur eines Unternehmens dar, wie beispielsweise eine Direktion, eine Abteilung oder einen Arbeitsplatz. Sie wird auf einer mehr oder weniger genauen Ebene definiert, je nachdem, wie präzise die Angaben über die Organisation sein müssen (siehe Organisationseinheitstyp). Beispiel: Finanzdirektion, Vertrieb, Marketingabteilung, Vertriebsmitarbeiter. Eine externe Entität stellt eine Einrichtung dar, die Flüsse mit dem Unternehmen austauscht. Beispiel: Kunde, Lieferant, Administration.

- *Geschäftsprozesse* und *organisatorische Prozesse*, bei denen Risiken bestehen.

  Ein Geschäftsprozess stellt ein System dar, das Produkte oder Dienstleistungen an einen internen oder externen Kunden des Unternehmens oder Organisation liefert. Auf höherer Ebene definiert ein Geschäftsprozess eine Strukturierung und Kategorisierung des Geschäftsbereichs eines Unternehmens. Der Geschäftsprozess kann in weitere Prozesse unterteilt werden. Mit der Verbindung zu den organisatorischen Prozessen kann die reelle Implementierung des Geschäftsprozesses in der Organisation beschrieben werden. Ein



Geschäftsprozess kann auch mit einer funktionalen Sicht detailliert werden.

Ein organisatorischer Prozess beschreibt die Schritte, die durchgeführt werden müssen, um den Prozess zur Herstellung eines Produkts oder Flusses insgesamt oder teilweise umzusetzen.

- *Ziele* und *Anforderungen*, die gegenüber dem Risikomanagement erwartet werden.

  Ein Ziel ist ein Ergebnis, das erreicht werden soll, oder das angestrebte Resultat eines Prozesses oder eines Arbeitsschritts. Mit einem Ziel können die Punkte hervorgehoben werden, die für diesen Prozess oder diesen Arbeitsschritt verbessert werden sollen.

  Eine Anforderung ist ein explizit ausgedrückter Bedarf oder eine Erwartung, die wie eine Einschränkung vorgeschrieben und im Rahmen eines Zertifikations-, Organisations- oder Modifikationsprojekts für das Informationssystem des Unternehmens erfüllt werden muss.

Risiko analysieren

Mit einer Risikoanalyse soll das Risiko gut verstanden werden.

In der Risikoanalyse müssen die Risikoquellen sowie die positiven und negativen Folgen bzw. Konsequenzen dieses Risikos berücksichtigt werden. Bei einer Analyse werden Ursachen, Ereignistypen, Risikofaktoren und Folgen mit einem Risiko verbunden.

Um ein Risiko zu analysieren, gehen Sie wie folgt vor:

1. Wählen Sie ein Risiko aus und öffnen Sie die Eigenschaftsseite des Risikos.
2. Klappen Sie in der Registerkarte **Merkmale** auf der Seite des Risikos den Abschnitt **Analyse** auf.
   Ein Risiko zeichnet sich wie folgt aus:
   - durch **Risikotypen**. Weitere Informationen finden Sie unter "Die Risikotypen", Seite 33.

     Ein Risikotyp definiert die Typologie eines normalisierten Risikos im Rahmen einer Organisation.
   - durch **Risikofaktoren**. Weitere Informationen finden Sie unter "Risikofaktoren", Seite 34.

     Ein Risikofaktor ist ein Element, das zum Auftreten eines Risikos beiträgt oder ein Risiko auslöst. Für verschiedene Risiken kann ein und derselbe Risikofaktor verantwortlich sein. Beispiele: Die Verwendung eines gefährlichen chemischen Produkts, eine komplexe Anwendung, die Größe eines Projekts, die Anzahl der Mitwirkenden, eine neue Technik, mangelnde Qualitätssicherung, mangelnde Sorgfalt bei der Festlegung der Anforderungen usw.
   - durch **Folgen eines Risikos**: Ausführliche Informationen finden Sie unter "Die Folgen eines Risikos", Seite 34.

     Die Folge eines Risikos kann positiv oder negativ sein. Sie wird mit einem Typ verbunden, mit dem sich die Folge charakterisieren lässt. Beispiel: Bild, Umgebung, Angestellte.

Die Risikotypen

Unternehmen sind oft zahlreichen *Risikotypen* ausgesetzt: Finanzwesen, Recht, Umwelt, IT, Technik, Vertrieb, usw.

Ein Risikotyp definiert die Typologie eines normalisierten Risikos im Rahmen einer Organisation.

Diese *Risiken* lassen sich durch die zunehmend komplexen Systemstrukturen (Ausfallrisiken), durch die Globalisierung des Welthandels (keine Kontrolle mehr über die Mitwirkenden), durch den Wettbewerb (schnelle Reaktion auf Ereignisse notwendig), usw. erklären.

Eine *Risikotyp* charakterisiert ein Risiko. Risikotypen können vorschriftsmäßiger, rechtlicher, technischer Art sein. Die Zusammensetzung eines Risikotyps hängt von den verschiedenen Aktivitäten und den Geschäftssparten oder besonderen Aktivitäten des Unternehmens ab. Die allgemeinen Risikotypen können sich mehr oder weniger aus spezifischen Risikotypen zusammensetzen.

Es ist wichtig, einen Risikotyp so zu definieren, dass er sich identifizieren, messen und verwalten lässt. Ebenso muss die Anzahl der verschiedenen Risikostufen begrenzt werden, um eine nützliche Nomenklatur zu erhalten.

Mit der Freigabe der Nomenklatur muss sichergestellt werden, dass ein Risikotyp, der in zwei verschiedenen Entitäten oder Aktivitäten definiert wurde, dieselbe Definition und dieselbe Bedeutung hat, um ein kohärentes System zu erhalten.

Da dieses System ebenfalls den Vorschriften genügen muss, muss eine zweite Nomenklatur definiert werden, um die deklarativen Aspekte zu berücksichtigen und um dem Informationsaustausch mit den Kontrollsystemen zu genügen.

`Beispielsweise wurden im Bankenbereich die Risikotypen im Rahmen der Empfehlungen von Basel II definiert. Weitere Informationen finden Sie unter http://www.bis.org/bcbs/.`

Um eigene Risikotypen zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie im Navigationsfenster **Umgebung > Risikouniversum > Risiken > Risikotypen** aus.
2. Klicken Sie im Kontextmenü des Ordners "Risikotyp" auf den Befehl **Neu**.
3. Geben Sie den Namen des Risikotyps ein und klicken Sie auf **OK**.
   In der Baumstruktur des Navigators wird der neue Risikotyp angezeigt.

☛ *Auf gleiche Weise können Sie ab einem Risikotyp einen Risikountertyp erstellen.*

Risikofaktoren

Viele *Risikofaktoren* werden im Rahmen internationaler, nationaler Bestimmungen, Vorschriften innerhalb verschiedener Berufsverbände oder im Unternehmen selbst definiert.

Ein Risikofaktor ist ein Element, das zum Auftreten eines Risikos beiträgt oder ein Risiko auslöst. Für verschiedene Risiken kann ein und derselbe Risikofaktor verantwortlich sein. Beispiele: Die Verwendung eines gefährlichen chemischen Produkts, eine komplexe Anwendung, die Größe eines Projekts, die Anzahl der Mitwirkenden, eine neue Technik, mangelnde Qualitätssicherung, mangelnde Sorgfalt bei der Festlegung der Anforderungen usw.

Jedem Risiko können ein oder mehrere *Risikofaktoren* zugeordnet werden, die Risikoquellen oder Gefahren darstellen, die den Betrieb der Organisation potenziell

gefährden können. Beispiel: gefährliche chemische Produkte, Konkurrenten, Regierungen usw..

Die Folgen eines Risikos

Die Folge eines Risikos kann positiv oder negativ sein. Sie wird mit einem Typ verbunden, mit dem sich die Folge charakterisieren lässt. Beispiel: Bild, Umgebung, Angestellte.

Um die Folgen eines Risikos zu definieren, gehen Sie wie folgt vor:

- Klicken Sie auf der Seite eines Risikos, im Abschnitt **Analyse**, Registerkarte **Risikofolgen** auf die Schaltfläche **Neu**.
  Daraufhin wird die Seite zum Erstellen einer Folge geöffnet.

  ☛ *Eine Risikofolge kann sich nur auf ein einziges Risiko beziehen. Daher ist das aktuelle Risiko im Feld **Risiko** bereits angegeben.*

Im Abschnitt **Risikofolgen** können Sie den **Identifizierungscode** der Folge angeben.

Die erstellte Folge wird in der Liste der Folgen des betreffenden Risikos aufgeführt.

Verantwortungsbereich eines Risikos festlegen

Sie können den oder die Verantwortlichen für das Risikomanagement im Abschnitt **Verantwortung** angeben.

☛ *Weitere Informationen zur Verwaltung der Verantwortung im Rahmen von RACI finden Sie im Handbuch **HOPEX Solutions Common Features**.*

Prozess der Erstellung eines Risikos

Der Prozess einer Risikoerstellung wird von einem Workflow verwaltet. Nur bestimmte Profile dürfen ein Risiko erstellen, einreichen, freigeben oder zurückweisen.

☛ *Weitere Informationen zum Workflow beim Erstellen eines Risikos und zu den entsprechenden E-Mails zur Benachrichtigung finden Sie unter "Workflow eines Risikos", Seite 104.*

Risiko erstellen

Nur Risikomanager und funktionale Administratoren dürfen Risiken erstellen.

Um ein Risiko zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie **Risiko** > **Risikobibliothek > Risiken > Risiken > Alle Risiken** aus.
   Daraufhin wird die Liste aller Risiken angezeigt.
2. Klicken Sie auf die Schaltfläche **Neu**.
   Daraufhin wird die Seite zum Erstellen eines Risikos angezeigt.

3. Geben Sie den **Namen** des Risikos an und klicken Sie auf **OK**.
   Das erstellte Risiko wird in der Liste der Risiken mit dem Status "Erstellt" aufgeführt.
4. Öffnen Sie die Eigenschaftsseite des Risikos.
5. Geben Sie den **Eigentümer** des Risikos an, der die weiteren Informationen zu dem neuen Risiko eingeben muss, bevor er das Risiko zur Freigabe einreicht.

Risiko duplizieren

Wenn ein Risiko dupliziert wird, können alle Eigenschaften eines existierenden Risikos kopiert werden.

Um ein Risiko zu duplizieren, gehen Sie wie folgt vor:

- Klicken Sie auf das zu duplizierende Risiko und klicken Sie wählen Sie den Befehl **Duplizieren** aus.
  In der Liste der Risiken wird ein neues Risiko mit demselben Namen wie das ursprüngliche Risiko aufgeführt.

Das duplizierte Risiko ist mit dem ursprünglichen Risiko identisch: Alle Merkmale und Verbindungen zu den anderen Objekten im Repository sind identisch. Die Aktionspläne wurden dupliziert. Nur eventuelle Bewertungsmaßnahmen für das Risiko wurden nicht dupliziert.

Risiko freigeben

Schritte des Freigabeprozesses eines neuen Risikos:

- Nachdem er die Merkmale eines neuen Risikos angegeben hat, kann der Ersteller eines Risikos (der ebenfalls der Eigentümer ist):
  - das Risiko **einreichen** .
  Der Risikomanager erhält per E-Mail eine Benachrichtigung. Das neue Risiko wird mit dem Status "Eingereicht" aufgeführt.
- Wenn das Risiko vom Eigentümer eingereicht wird, kann der Risikomanager:
  - das Risiko **freigeben**. Das Risiko übernimmt den Status "Freigegeben".
  Der Benutzer Eigentümer erhält per E-Mail eine Benachrichtigung.
  - das Risiko **zurückweisen**.
  In diesem Fall übernimmt das Risiko den Status "Zurückgewiesen", wird aber nicht gelöscht.

Risiken organisieren

Mit der Kontextualisierung eines Risikos werden Risiken nach Typ und nach den betroffenen Objekten klassiert. Ein Risiko kann mehrere Typen von Komponenten betreffen:

- **Entitäten**
- **Prozesse**, **Geschäftsprozesse** und **organisatorische Prozesse**
- **Ziele**

In **MEGA ERM** können Risiken und die entsprechenden Objekte einfach verbunden werden.

Standardmäßig sind Berichte über die Kontextualisierung der Risiken verfügbar. Weitere Informationen finden Sie unter "Kreuztabelle einer Aufteilung", Seite 82.

Auf Risiken ab Kontext zugreifen

Um die Liste der Risiken abhängig von ihrem Kontext zu erhalten, gehen Sie wie folgt vor:

1. Wählen Sie **Risiko** > **Risikobibliothek > Baumstruktur von Risiken** aus.
   Daraufhin wird die Liste der Ordner mit den Klassierungen der Risiken angezeigt.
2. Sie können die Baumstruktur aufklappen, um die Liste der Risiken eines Objekts anzuzeigen.



Risiken kontextualisieren

In **MEGA ERM** können Risiken und die entsprechenden Objekte einfach verbunden werden: eine *Entität*, ein *Prozess* oder ein *Ziel*.

Um die Risiken zu kontextualisieren, gibt es drei Möglichkeiten:

- eine Darstellung in Form einer Liste verwenden
- eine Darstellung in Form einer Baumstruktur verwenden
- eine Darstellung in Form einer Kreuztabelle verwenden

Listen für die Kontextualisierung eines Risikos verwenden

Um eine Liste der Risiken mit einem Objekt zu verbinden, gehen Sie wie folgt vor:

1. Wählen Sie **Risiko** > **Risikobibliothek > Kontextualisierung> Listenansicht** aus.
   Die Liste der Risiken wird links neben der Bearbeitungszone angezeigt, die Baumstrukturen der Kontextualisierung rechts.
2. Wählen Sie einen Bereich von Objekttypen aus, zum Beispiel **Risiken nach Entitäten** und klappen Sie die Baumstruktur auf, bis die Entität angezeigt wird, die für Sie von Interesse ist.
3. Wählen Sie im linken Teil der Bearbeitungszone die relevanten Risiken aus.
4. Halten Sie die rechte Maustaste gedrückt und verschieben Sie die ausgewählten Risiken unter die Entität, mit der sie verbunden werden sollen.
   Die Liste der ausgewählten Risiken wird rechts unter der gewählten Entität angezeigt.

Baumstrukturen für die Kontextualisierung eines Risikos verwenden

Mit den Baumstrukturen für die Kontextualisierung können Sie eine gewisse Kohärenz zwischen den Risiken sicherstellen, die mit verschiedenen Objekttypen verbunden sind.

Sie können zum Beispiel Risiken bei einem organisatorischen Prozess mit der Entität verbinden, die für die Umsetzung dieses Prozesses verantwortlich ist:

1. Wählen Sie **Risiko** > **Risikobibliothek > Kontextualisierung > Kontextualisierung > Hierarchische Ansicht** aus.
   Rechts und links werden neben der Bearbeitungszone zwei Baumstrukturen einer Kontextualisierung werden.
2. Wählen Sie in der rechten Baumstruktur der Kontextualisierung beispielsweise **Risiken nach Prozessen** aus und klappen Sie die Baumstruktur auf, bis die Risiken angezeigt werden, die mit dem Prozess verbunden sind, der für Sie von Interesse ist.
3. Wählen Sie in der linken Baumstruktur der Kontextualisierung **Risiken nach Entitäten** aus und klappen Sie die Baumstruktur auf, bis die Entität angezeigt wird, die für Sie von Interesse ist.
4. Klicken Sie mit der linken Maustaste auf das gewünschte Risiko, halten Sie die Maustaste gedrückt und verschieben Sie das ausgewählte Risiko zur Entität, mit der er verbunden werden soll.

Kreuztabelle für die Kontextualisierung eines Risikos verwenden

Sie können eine Kreuztabelle verwenden, um Risiken mit Entitäten oder Prozessen zu verbinden.

Um Risiken mit Entitäten zu verbinden, gehen Sie wie folgt vor:

1. Wählen Sie **Risiko** > **Risikobibliothek > Kontextualisierung > Kreuztabellenkontextualisierung > Risiken nach Entitäten** aus.
   In der Bearbeitungszone wird ein leerer Bericht angezeigt.
2. Klicken Sie in der Bearbeitungszone oben auf den Befehl **Zeile hinzufügen**
   Das Abfragefenster wird angezeigt.
3. Klicken Sie auf die Schaltfläche **Abfragen**.
   Im Abfragefenster wird die Liste der Risiken aufgeführt.
4. Wählen Sie die gewünschten Risiken aus und klicken Sie auf **OK**.
   Die ausgewählten Risiken werden in der Bearbeitungszone in Zeilen angezeigt.
5. Gehen Sie genauso vor, um die Entitäten auszuwählen, und klicken Sie auf den Befehl **Spalte hinzufügen**.
   Die ausgewählten Entitäten werden in der Bearbeitungszone in Spalten angezeigt.
6. Wenn Sie am Schnittpunkt eines Risikos und einer Entität auf das leere Kästchen klicken, wird das Risiko mit der Entität verbunden.
   Im Kästchen wird das Symbol angezeigt.

   ☛ *Gehen Sie genauso vor, um die Verbindung eines Risikos mit einer Entität zu trennen.*

ÜBERWACHUNG DER KONTROLLPOLITIK

Die Kontrollaktivitäten bestehen aus Strategien und Abläufen, mit denen sichergestellt wird, dass die von der Geschäftsleitung gewünschten Risikoreaktionen tatsächlich eingerichtet wurden.

Die Überwachung erfolgt durch permanente Aktivitäten des Managements oder durch unabhängige Beurteilungen oder aber auch durch eine Kombination beider Modalitäten.

Standardmäßig sind Berichte über die Kontextualisierung der Kontrollen verfügbar. Weitere Informationen finden Sie unter "Identifizierung der Kontrollen", Seite 86.

KONTROLLEN VERWALTEN

Mit der Risikoidentifikation und -analyse konnte eine Reihe von Risiken ermittelt werden, gegen die man sich nun wappnen muss. Kontrolltätigkeiten müssen definiert werden, mit denen diese Risiken und ihre möglichen Folgen vermieden werden können.

Diese *Kontrollen* müssen formell festgelegt werden, um Vorschriften zu erfüllen, wie beispielsweise das Gesetz Sarbanes-Oxley, oder die Empfehlungen von Basel II für das Bankwesen.

Eine Kontrolle ist ein Mittel, ein oder mehrere Risiken unter Kontrolle zu haben, und sicherzustellen, dass eine gesetzliche, vorschriftsmäßige oder interne Anforderung des Unternehmens erfüllt wird.

In **MEGA ERM** existieren verschiedene Objekttypen, die mit Kontrollen verbunden sind:

- Objekttypen, mit denen angegeben wird, in welchem Rahmen diese Kontrolle eingerichtet wird (Kontrolleinrichtung, Kontrolltyp, Anforderung oder verbundenes Risiko)
- Objekttypen, mit denen die Mittel zur Umsetzung dieser Kontrolle angegeben werden (organisatorischer Prozess, Anwendung usw.).
- Objekttypen, mit denen die Verantwortungen bei der Umsetzung dieser Kontrolle angegeben werden (Entitäten, Benutzer).

Zugriff auf die Kontrollen

Genauso wie die Risiken können auch die Kontrollen, die mit diesen Risiken verbunden sind, sehr zahlreich sein. Um die Verwaltung dieser Kontrollen besser zu handhaben, bietet **MEGA ERM** mehrere Möglichkeiten für den Zugriff auf die Liste der Kontrollen.

- Entweder wählen Sie **Risiko** > **Risikobibliothek > Risiken > Kontrollen> Alle Kontrollen** aus oder
- Sie wählen **Risiko > Bearbeitung > Kontrollen > Alle Kontrollen** aus.

Objekte der Kontrolle

Im Allgemeinen sollten zuerst die existierenden Kontrollen erfasst werden, bevor neue erstellt eingerichtet werden.

Vor diesem Hintergrund können die Kontrollen auf verschiedene Weisen identifiziert werden:

- ab Risiken
  Einige Kontrollen werden für ein bestimmtes Risiko eingerichtet.
- ab Listen von Kontrolltypen
  Die Listen der Kontrolltypen werden mit bestimmten Vorschriften verbunden (Beispiel: Cobit).
- ab einer Kartografie der existierenden Prozesse
  wenn diese Kartografie verfügbar ist, kann genau wie bei der Identifizierung von Risiken geprüft werden, wie die einzelnen Schritte eines Prozesses funktionieren, um die eingerichteten Kontrollen zu entdecken.
- ab der Expertise eines Spezialisten
  Ein Fachmann oder Spezialist eines bestimmten Bereichs kann oft die Kontrollen beschreiben, die eingerichtet sind oder eingerichtet werden müssen.
- usw.

Sie können eine Kontrolle genauer definieren und den Kontrolltyp, die Anforderungen, die Risiken und Risikofaktoren angeben, die mit der Kontrolle verbunden sind.

Dazu gehen Sie wie folgt vor:

1. Wählen Sie die Kontrolle in der Liste aus und öffnen Sie die Eigenschaftsseite der Kontrolle.
2. Klappen Sie den Abschnitt **Umfang** auf.
   - In den Registerkarten **Geschäftsprozess** und **organisatorischer Prozess** können Sie die *Prozesse* angeben, mit denen die Kontrolle durchgeführt wird.

     Ein Prozess ist eine Wertekette, die einem internen oder externen Kunden Güter oder Services bereitstellt. Diese Wertekette wird durch eine Folge von Aktivitätsumwandlungen beschrieben. Sie wird von den Abläufen implementiert.
   - In der Registerkarte **Entität** können Sie die Entitäten angeben, mit denen die Kontrolle durchgeführt wird.

     Eine Entität kann unternehmensintern oder -extern sein: Eine Entität stellt ein Element der Struktur eines Unternehmens dar, wie beispielsweise eine Direktion, eine Abteilung oder einen Arbeitsplatz. Sie wird auf einer mehr oder weniger genauen Ebene definiert, je nachdem, wie präzise die Angaben über die Organisation sein müssen (siehe Organisationseinheitstyp). Beispiel: Finanzdirektion, Vertrieb, Marketingabteilung, Vertriebsmitarbeiter. Eine externe Entität stellt eine Einrichtung dar, die Flüsse mit dem Unternehmen austauscht. Beispiel: Kunde, Lieferant, Administration.
   - In der Registerkarte **Risiken** können Sie angeben, welche *Risiken* durch die Kontrolle vermieden werden.Ein Risikotyp definiert die Typologie eines normalisierten Risikos im Rahmen einer Organisation.

     Ein Risikofaktor ist ein Element, das zum Auftreten eines Risikos beiträgt oder ein Risiko auslöst. Für verschiedene Risiken kann ein und derselbe Risikofaktor verantwortlich sein. Beispiele: Die Verwendung eines gefährlichen chemischen Produkts, eine komplexe Anwendung, die Größe eines Projekts, die Anzahl der Mitwirkenden, eine neue Technik,

mangelnde Qualitätssicherung, mangelnde Sorgfalt bei der Festlegung der Anforderungen usw.

- In der Registerkarte **Anforderungen** können Sie angeben, welcher vorschriftsmäßigen oder gesetzlichen *Anforderung* die Kontrolle entspricht.

  Eine Anforderung ist ein explizit ausgedrückter Bedarf oder eine Erwartung, die wie eine Einschränkung vorgeschrieben und im Rahmen eines Zertifikations-, Organisations- oder Modifikationsprojekts für das Informationssystem des Unternehmens erfüllt werden muss.

- In der Registerkarte **Kontrolltyp** können Sie angeben, auf welche Kontrolltypen die Kontrolle verweist.

  Mit einem Kontrolltyp lassen sich die Kontrollen klassieren, die im Unternehmen entsprechend des Standards bzw. Normen der betreffenden Sektoren oder Vorschriften/Reglementierungen (Cobit usw.) implementiert sind.

Kontrolle analysieren

Mit dem oder den *Kontrolltypen* werden die Vorschriften angegeben, die für eine Kontrolle gelten.

Mit einem Kontrolltyp lassen sich die Kontrollen klassieren, die im Unternehmen entsprechend des Standards bzw. Normen der betreffenden Sektoren oder Vorschriften/Reglementierungen (Cobit usw.) implementiert sind.

Diese Kontrollen können definiert werden, indem die Kontrolltypen berücksichtigt werden, die im Rahmen des betroffenen Kontroll- und Risikosystems festgelegt wurden.

Ein Kontrollsystem besteht aus mehreren Kontrollen, mit denen Risiken für ein Unternehmen verhütet und Risiken unter Kontrolle gehalten werden können, sowie interne Betriebsregeln angewendet, Gesetze oder Vorschriften eingehalten oder strategische Ziele des Unternehmens erreicht werden können.

Dieses Kontrollsystem entspricht der Umsetzung einer Vorschrift in einem der Geschäftsbereiche des Unternehmens, wie beispielsweise die Anwendung einer Finanzpolitik im Unternehmen im Bereich Einkauf.

Um auf die Kontrolltypen zuzugreifen, gehen Sie wie folgt vor:

- Wählen Sie **Risiko** > **Risikobibliothek > Risiken > Kategorien > Kontrolltypen** aus.
  Es wird eine Liste der Kontrolltypen angezeigt.

Verantwortungsbereiche von Kontrollen festlegen

Sie können den oder die Verantwortlichen für die Umsetzung der Kontrolle im Abschnitt **RACI** angeben.

☛ *Weitere Informationen zur Verwaltung der Verantwortung im Rahmen von RACI finden Sie im Handbuch **HOPEX Solutions Common Features**.*

KONTROLLE ERSTELLEN

Der Prozess der Erstellung einer Kontrolle wird von einem Workflow verwaltet. Nur bestimmte Profile dürfen eine Kontrolle erstellen, einreichen, freigeben oder zurückweisen.

☛ *Weitere Informationen zum Workflow beim Erstellen eines Risikos und zu den entsprechenden Benachrichtigungen finden Sie unter* *"Workflow einer Kontrolle", Seite 106.*

Kontrolle erstellen

Nur Risikomanager und funktionale Administratoren dürfen Kontrollen erstellen.

Um eine Kontrolle zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie **Risiko** > **Risikobibliothek > Risiken > Kontrollen > Alle Risiken** aus.
   Daraufhin wird die Liste aller Kontrollen angezeigt.
2. Klicken Sie auf die Schaltfläche **Neu**.
   Die erstellte Kontrolle wird in der Liste der Kontrollen mit dem Status "Erstellt" aufgeführt.
3. Öffnen Sie das Eigenschaftsfenster der Kontrolle.
4. Geben Sie den **Eigentümer** der Kontrolle an, der die weiteren Informationen zur neuen Kontrolle eingeben muss, bevor er die Kontrolle zur Freigabe einreicht.

Kontrolle freigeben

Schritte des Freigabeprozesses einer neuen Kontrolle:

- Nachdem er die Merkmale einer neuen Kontrolle angegeben hat, kann der Eigentümer der Kontrolle:
  - die Kontrolle **einreichen** . Die neue Kontrolle wird mit dem Status "eingereicht" angezeigt.

  Der Risikomanager erhält eine Benachrichtigung per E-Mail.
- Wenn eine Kontrolle vom Eigentümer eingereicht wurde, kann der Risikomanager:
  - die Kontrolle **freigeben**. Die Kontrolle übernimmt den Status "Freigegeben".

  Der Benutzer "Eigentümer" erhält per E-Mail eine Benachrichtigung.
  - die Kontrolle **zurückweisen** .

  In diesem Fall übernimmt die Kontrolle den Status "Zurückgewiesen", wird aber nicht gelöscht.

BEWERTUNGEN MIT MEGA ERM

Nach der Identifizierung und Analyse der Risiken für ein Unternehmen, müssen die wichtigsten Risiken herausgestellt werden, um sie bearbeiten zu können. In **MEGA ERM**, werden Risiken qualitativ bewertet: die Auswirkung eines Risikos wird nur mit Begriffen beschrieben, die einer vordefinierten Skala entsprechen (zum Beispiel von 1 bis 4). So kann eine Risikokartografie erstellt werden, mit der die kritischsten Risiken schnell identifiziert werden können.

MEGA ERM bietet zwei Bewertungsmöglichkeiten an:

- die direkte Bewertung, mit der ein Experte die globale Bewertung eines Risikos zu einem bestimmten Datum aufstellen kann.
- die Bewertung nach Kampagnen, mit der Risiken und Kontrollen nach Entitäten und nach Prozessen ab Standardfragebögen bewertet werden können.

In diesem Kapitel werden folgende Punkte behandelt:

DIREKTE BEWERTUNG DER RISIKEN

Die Bewertung der Risiken und Kontrollen erfolgt qualitativ: die Potenzialität und Auswirkung eines Risikos werden nur mit Begriffen beschrieben (Beispiel: sehr gering, gering, mittel, sehr hoch, hoch).

Bei diesen Bewertungen wird das Konzept der Risikobemessung genutzt. Risikomessungen werden erstellt, um zu einem bestimmten Datum die Risikobewertung einer Entität oder eines Prozesses der Organisation zu liefern. Auf der Eigenschaftsseite eines Risikos können Sie die verschiedenen bereits durchgeführten Risikomessungen aufrufen.

Diese Messungen werden zum Erstellen von Standardberichten verwendet, mit denen sich Risiken nach der Bewertung einfacher analysieren lassen.

Zugriff auf die Ergebnisse der Risikobewertung

Die Ergebnisse der Risikobewertung können in angepassten Berichten aufgeführt werden, mit denen sich die bewerteten Risiken einfacher analysieren lassen.

- "Die Aggregationen", Seite 87
- "Effizienz des Risikomanagements", Seite 95
- "Trendanalyse", Seite 96

Die Kreuztabelle der direkten Bewertung ist ein einfaches Mittel, die Bewertungsergebnisse spezieller Risiken aufzurufen.

Zugriff auf die Kreuztabelle einer direkten Bewertung der Risiken

Um auf die Kreuztabelle einer direkten Bewertung der Risiken zuzugreifen, gehen Sie wie folgt vor:

1. Klicken Sie auf den Befehl **Risiko** > **Risikobibliothek > Direkte Bewertung > Mehrfachbewertungstabelle**.
   In der Bearbeitungszone wird eine leere Tabelle angezeigt.
2. Klicken Sie auf den Befehl **Zu bewertende Risiken verbinden**
   Die Liste der Risiken wird in einem neuen Fenster aufgeführt.

3. Wählen Sie die gewünschten Risiken aus und klicken Sie auf **Verbinden**. Die ausgewählten Risiken werden in der Bearbeitungszone in Zeilen angezeigt. Die Maße der letzten Risikomessung werden in Spalten angezeigt.



Local name	Impact	Likelihood	Inherent Risk	Mitigation Design	Mitigation Efficiency	Mitigation Level	Net Risk
Application Hack	Medium	Rare	Low	Weak	Very Strong	Strong	Low
Change risks	Very Low	Possible	Low	Medium	Medium	Medium	Mediur
Contractual risks	High	Likely	High	Strong	Strong	Strong	Mediur
Counterparty risks	High	Probable	High	Very Strong	Very Strong	Very Strong	Low
Cut-off	Medium	Likely	Medium	Medium	Medium	Medium	Mediur
Default of payment	High	Probable	High	Medium	Very Weak	Weak	High
Fraud & Corruption	Very Low	Probable	Low	Weak	Very Weak	Very Weak	High

Maße der Risikomessungen:

- **Auswirkung**: bezeichnet die Auswirkung des Risikos, wenn es eintritt.
- **Wahrscheinlichkeit**: bezeichnet die Wahrscheinlichkeit, dass das Risiko eintritt.
- **Bruttorisiko**: das Ergebnis des Auswirkunsgwerts multipliziert mit dem Wert der Wahrscheinlichkeit. Dieses Merkmal gibt Aufschluss über die Folgen des Risikos.
- **Design der Kontrollen**: bezeichnet die Aktionen, mit denen der Eintritt eines Risikos oder seine Folgen reduziert werden.
- **Wirksamkeit der Kontrollen**: bezeichnet die Effizienz der eingeleiteten Aktionen, mit denen der Eintritt eines Risikos oder seine Folgen reduziert werden sollen
- **Kontrollebene**: ist das Ergebnis des Werts des Designs der Kontrollen multipliziert mit dem Wert der Auswirkung der Kontrollen. Dieses Merkmal gibt einen globalen Aufschluss darüber, inwieweit das Risiko unter Kontrolle ist.
- **Nettorisiko**: die Differenz zwischen dem **Bruttorisiko** und der **Kontrollebene**.

Zugriff auf die Risikomessungen

Mit einer Risikomessung sollen in einem bestimmten Kontext Werte für die verschiedenen Maße erhalten werden, wie zum Beispiel die Wahrscheinlichkeit oder die Auswirkung eines Risikos.

Auf der Eigenschaftsseite eines Risikos können Sie die verschiedenen bereits durchgeführten Risikomessungen aufrufen.

Die Werte für die Maße können angegeben werden:

- ab der Eigenschaftsseite eines Risikos. Weitere Informationen finden Sie unter "Kreuztabelle der direkten Bewertung verwenden", Seite 51
- ab der Kreuztabelle der Risikobewertung. Weitere Informationen finden Sie unter "Risikomessung erstellen", Seite 50
- oder über ein Bewertungsformular. Weitere Informationen finden Sie unter "Bewertung nach Fragebögen", Seite 53.

Um auf die Risikomessungen zuzugreifen, gehen Sie wie folgt vor:

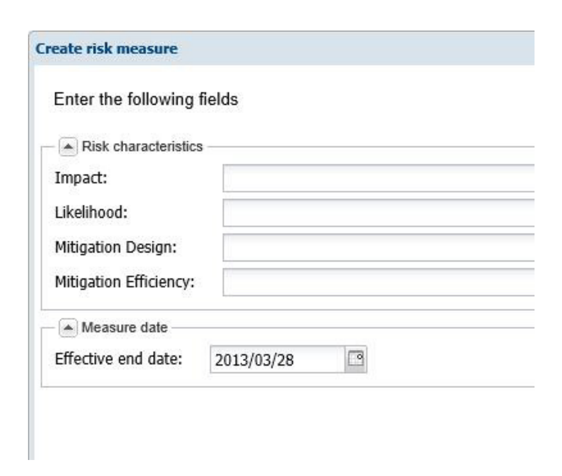
1. Wählen Sie ein Risiko aus und öffnen Sie die Eigenschaftsseite des Risikos.
2. Klicken Sie auf die Registerkarte **Bewertung**.
   Die Liste der Risikomessungen wird angezeigt.

Risikomessung erstellen

Sie können neue Risikomessungen erstellen, um bei mehreren Objekten der Organisation ein Risiko global zu bewerten, das mit den Objekten verbunden ist (Entitäten und Prozesse).

Um eine Risikomessung zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie ein Risiko aus und öffnen Sie die Eigenschaftsseite des Risikos.
2. Klicken Sie auf die Registerkarte **Bewertung** des Risikos.
3. Klicken Sie auf die Schaltfläche **Neu**.



4. Geben Sie die Werte an:

- **Auswirkung**: bezeichnet die Auswirkung des Risikos, wenn es eintritt.
  - "Sehr schwach"
  - "Schwach"
  - "Mittel"
  - "Sehr hoch"
  - "Erhöht"
- **Wahrscheinlichkeit**: bezeichnet die Wahrscheinlichkeit, dass das Risiko eintritt.
  - "Schwach"
  - "Möglich"
  - "Vermutlich"
  - "Wahrscheinlich"
  - "Bestimmt"
- **Design der Kontrollen**: bezeichnet die Aktionen, mit denen der Eintritt eines Risikos oder seine Folgen reduziert werden.
  - "Sehr stark"
  - "Stark"
  - "Mittel"
  - "Schwach"
  - "Sehr schwach"
- **Wirksamkeit der Kontrollen** : bezeichnet die Effizienz der eingeleiteten Aktionen.
  - "Sehr stark"
  - "Stark"
  - "Mittel"
  - "Schwach"
  - "Sehr schwach"

5. Geben Sie das Datum der Risikomessung an.
6. Klicken Sie auf **OK**.

Kreuztabelle der direkten Bewertung verwenden

Sie können die Werte für die Risikomessung direkt in einer Kreuztabelle ändern.

Um die Werte für die Risikomessung anzugeben, gehen Sie wie folgt vor:

1. Klicken Sie auf den Befehl **Risiko** > **Risikobibliothek > Direkte Bewertung > Mehrfachbewertungstabelle**.
   In der Bearbeitungszone wird eine leere Tabelle angezeigt.
2. Klicken Sie auf den Befehl **Zu bewertende Risiken verbinden**
   Die Liste der Risiken wird in einem neuen Fenster aufgeführt.
3. Wählen Sie die gewünschten Risiken aus und klicken Sie auf **Verbinden**.
   Die ausgewählten Risiken werden in der Bearbeitungszone in Zeilen angezeigt. Die Maße der Risikomessungen werden in Spalten angezeigt.

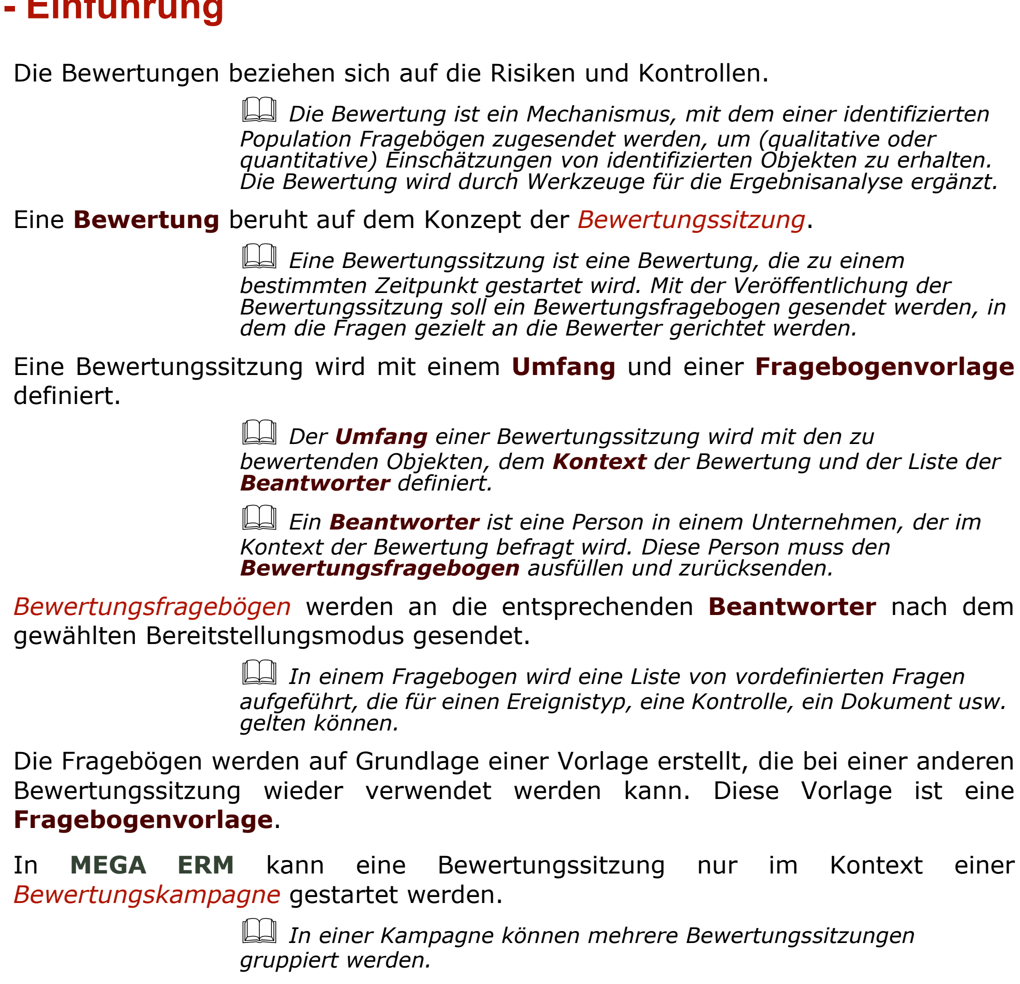
4. Klicken Sie auf das Kästchen, das für ein bestimmtes Risiko einem Maß entspricht, zum Beispiel auf **Auswirkung**.
   Nun wird die Liste der möglichen Werte angezeigt.
5. Wählen Sie den gewünschten Wert aus.
6. Klicken Sie anschließend auf den Befehl **Bewertung freigeben**.
7. Geben Sie das Datum der Bewertung ein und klicken Sie auf **OK**.
   Die neue Risikomessung ist nun erstellt.

BEWERTUNG NACH FRAGEBÖGEN

In **MEGA ERM** können Sie ab Standardfragebögen Risiken und Kontrollen bewerten. Dadurch können Sie die Leistung interner Kontrollsysteme steigern und Risiken minimieren.

Die Bewertungsfragebögen werden an die entsprechenden Empfänger mithilfe der persönlich anpassbaren Modi für die Bereitstellung gesendet.

Konzepte - Einführung



Die Bewertungen beziehen sich auf die Risiken und Kontrollen.

Die Bewertung ist ein Mechanismus, mit dem einer identifizierten Population Fragebögen zugesendet werden, um (qualitative oder quantitative) Einschätzungen von identifizierten Objekten zu erhalten. Die Bewertung wird durch Werkzeuge für die Ergebnisanalyse ergänzt.

Eine **Bewertung** beruht auf dem Konzept der *Bewertungssitzung*.

Eine Bewertungssitzung ist eine Bewertung, die zu einem bestimmten Zeitpunkt gestartet wird. Mit der Veröffentlichung der Bewertungssitzung soll ein Bewertungsfragebogen gesendet werden, in dem die Fragen gezielt an die Bewerter gerichtet werden.

Eine Bewertungssitzung wird mit einem **Umfang** und einer **Fragebogenvorlage** definiert.

*Der **Umfang** einer Bewertungssitzung wird mit den zu bewertenden Objekten, dem **Kontext** der Bewertung und der Liste der **Beantworter** definiert.*

*Ein **Beantworter** ist eine Person in einem Unternehmen, der im Kontext der Bewertung befragt wird. Diese Person muss den **Bewertungsfragebogen** ausfüllen und zurücksenden.*

Bewertungsfragebögen werden an die entsprechenden **Beantworter** nach dem gewählten Bereitstellungsmodus gesendet.

In einem Fragebogen wird eine Liste von vordefinierten Fragen aufgeführt, die für einen Ereignistyp, eine Kontrolle, ein Dokument usw. gelten können.

Die Fragebögen werden auf Grundlage einer Vorlage erstellt, die bei einer anderen Bewertungssitzung wieder verwendet werden kann. Diese Vorlage ist eine **Fragebogenvorlage**.

In **MEGA ERM** kann eine Bewertungssitzung nur im Kontext einer *Bewertungskampagne* gestartet werden.

In einer Kampagne können mehrere Bewertungssitzungen gruppiert werden.

Zugriff auf die Bewertungsfunktionen

Ka nach Benutzerprofil können Sie in unterschiedlichen Menüs auf die Bewertungsfunktion zugreifen.

Profil	Aktion	Menü
Funktionaler Administrator	- Rollen Personen im Unternehmen zuweisen. - Organisation definieren (Entitäten, Prozesse usw.) - Beantworter festlegen (die die Bewerter der Risiken für jede Entität sind)	Umgebung Administration
Risikomanager	- Bewertungskampagnen erstellen - Bewertungssitzungen erstellen Bewertungssitzungen verfolgen	Risiko > Kampagnenmanagement
Risikobewerter	- Fragebogen akzeptieren oder ablehnen - Fragebogen beantworten	Risiko > Home > Mein Desktop > Meine Verantwortungsbereiche > Meine Bewertungsfragebögen

Die Bewertungsvorlagen von MEGA ERM

Bevor Sie eine **Bewertungssitzung** erstellen, müssen Sie zuvor eine **Bewertungskampagne** und den Umfang der Kampagne erstellen.

Der Umfang einer **Bewertungssitzung** wird mit folgenden Angaben definiert:

- Die Liste der zu bewertenden Objekte mit den jeweils zu bewertenden Merkmalen
- Der **Bewertungskontext**: welche Entitäten, welche Prozesse usw.
- Die **Profile** der befragten Personen
- Die **Bewertungsperiode**

Dieser Umfang wird auf der Ebene einer Bewertungskampagne mit einer **Bewertungsvorlage** generisch definiert.

Eine Bewertungsvorlage dient als Vorlage zur Erstellung von Bewertungskampagnen und -sitzungen. Die Bewertungsvorlage legt den Umfang der Bewertung fest, sowie die zu verwendende Fragebogenvorlage und eventuell die Aggregationsschemen, die für die Auslegung der globalen Ergebnisse verwendet werden.

Alle Sitzungen einer Kampagne beziehen sich also auf einen global identischen Umfang.

☛ *Der Verantwortliche der Sitzung kann weiterhin Elemente aus dem speziellen Umfang einer Sitzung entfernen bzw. hinzufügen.*

Zugriff auf Bewertungsvorlagen

Standardmäßig werden in **MEGA ERM** mehrere Bewertungsvorlagen angeboten. Mit diesen Bewertungsvorlagen soll eine Bewertung der Risiken bei einer Entität oder einem Prozess erhalten werden.

Die Bewertung bezieht sich entweder nur auf Risiken oder auf die Risiken und Kontrollen dieser Risiken.

Um auf die Liste der Bewertungsvorlagen zuzugreifen, gehen Sie wie folgt vor:

- Klicken Sie auf **Risiko > Kampagnenmanagement > Leitung der Kampagnen > Vorbereitung > Bewertungsvorlagen**.
  Die Liste der Bewertungsvorlagen wird im Bearbeitungsfenster angezeigt.
  - Bewertung nur von Risiken - nach Entität
  - Bewertung nur von Risiken - nach Entität, nach Prozess
  - Bewertung der Risiken - nach Entität
  - Bewertung der Risiken - nach Entität, nach Prozess
  - Bewertung der Kontrollen - nach Entität
  - Bewertung der Kontrollen - nach Entität, nach Prozess

☛ Weitere Informationen zur Verwendung der Bewertungsvorlagen finden Sie unter *"Details der Bewertungsvorlagen von MEGA ERM", Seite 57.*

Die angebotenen Bewertungsvorlagen verwenden:

- **Bewertete Merkmale**
- **Vorlagen von Fragebögen**

Die bewerteten Merkmale

Ein bewertetes Merkmal legt fest, was bei einer Bewertung bewertet werden soll. Das Merkmal kann mit einer MetaClass verbunden werden, vor allem mit einem der MetaAttributs, zum Beispiel. Metaclasse Risiko, MetaAttribut: Wahrscheinlichkeit.

Um auf die Liste der bewerteten Merkmale zuzugreifen, die standardmäßig von **MEGA ERM** angeboten werden, gehen Sie wie folgt vor:

- Klicken Sie auf **Risiko > Kampagnenmanagement > Leitung der Kampagnen > Vorbereitung > Bewertete Merkmale**.
  Die Liste der Merkmale wird im Bearbeitungsfenster angezeigt.

Diese Merkmale beziehen sich auf den Wert der Attribute der Kontrollen oder den Wert der Attribute der Risiken.

Liste der Merkmale, die mit den Attributen der Kontrolle verbunden sind:

- **Design der Kontrolle**: bezeichnet die genauen Aktionen, die für die Kontrolle eingeleitet werden
- **Kontrollwirksamkeit**: bezeichnet die Effizienz der eingeleiteten Aktionen
- **Kontrollebene**: das Ergebnis des Wertes der Spezifizierung multipliziert mit dem Wert der Wirkung. Dieses Merkmal gibt Aufschluss über die Effizienz der Kontrolle.

Liste der Merkmale, die mit den Attributen der Risiken verbunden sind:

☛ *Bei den einzelnen Attributen kann sich das bewertete Merkmal auf den Bruttowert, den maximalen Wert oder den durchschnittlichen Wert beziehen.*

- **Auswirkung**: bezeichnet die Auswirkung des Risikos, wenn es eintritt.
- **Wahrscheinlichkeit**: bezeichnet die Wahrscheinlichkeit, dass das Risiko eintritt.
- **Bruttorisiko**: das Ergebnis des Auswirkunsgwerts multipliziert mit dem Wert der Wahrscheinlichkeit. Dieses Merkmal gibt Aufschluss über die Folgen des Risikos.
- **Design der Kontrollen**: bezeichnet die Aktionen, mit denen der Eintritt eines Risikos oder seine Folgen reduziert werden.
- **Wirksamkeit der Kontrollen**: bezeichnet die Effizienz der eingeleiteten Aktionen, mit denen der Eintritt eines Risikos oder seine Folgen reduziert werden sollen
- **Kontrollebene**: ist das Ergebnis des Werts des Designs der Kontrollen multipliziert mit dem Wert der Auswirkung der Kontrollen. Dieses Merkmal gibt einen globalen Aufschluss darüber, inwieweit das Risiko unter Kontrolle ist.
- **Nettorisiko**: die Differenz zwischen dem **Bruttorisiko** und der **Kontrollebene**.

Die Fragebogenvorlagen

Eine Fragebogenvorlage entspricht der Definition des Inhaltes eines Fragebogens: Fragegruppe, Fragen, einmalige oder mehrere Antworten und mögliche Antworten. Die Fragebogenvorlage kann mit der Präsentation eines Fragebogens verbunden werden, die die Anzeigeoptionen angibt. Die an die Bewerter gesendeten Fragebögen werden ab der Definition generiert, die in der Fragebogenvorlage geliefert wird.

Um auf die Liste der Fragebogenvorlagen zuzugreifen, die standardmäßig von **MEGA ERM** angeboten werden, gehen Sie wie folgt vor:

› Klicken Sie auf **Risiko > Kampagnenmanagement > Leitung der Kampagnen > Vorbereitung > Fragebogenvorlagen**.
Im Bearbeitungsfenster wird die Liste der Fragebogenvorlagen für jede Bewertungsvorlage angezeigt, der standardmäßig angeboten wird.

Diese Fragebogenvorlagen beziehen sich auf:

- die Bewertung nur von Risiken ab folgenden Merkmalen:
  - **Auswirkung**: bezeichnet die Auswirkung des Risikos, wenn es eintritt.
  - **Wahrscheinlichkeit**: bezeichnet die Wahrscheinlichkeit, dass das Risiko eintritt.
  - **Design der Kontrollen**: bezeichnet die Aktionen, mit denen der Eintritt eines Risikos oder seine Folgen reduziert werden.
  - **Wirksamkeit der Kontrollen**: bezeichnet die Effizienz der eingeleiteten Aktionen, mit denen der Eintritt eines Risikos oder seine Folgen reduziert werden sollen
- die Bewertung der Risiken, die mit Kontrollen verbunden sind, ab folgenden Merkmalen:
  - **Auswirkung**: bezeichnet die Auswirkung des Risikos, wenn es eintritt.
  - **Wahrscheinlichkeit**: bezeichnet die Wahrscheinlichkeit, dass das Risiko eintritt.
- die Bewertung von Kontrollen ab folgenden Merkmalen:
  - **Design der Kontrolle**: bezeichnet die Aktionen, mit denen der Eintritt eines Risikos oder seine Folgen reduziert werden.
  - **Kontrollwirksamkeit**: bezeichnet die Effizienz der eingeleiteten Aktionen, mit denen der Eintritt eines Risikos oder seine Folgen reduziert werden sollen.

Details der Bewertungsvorlagen von MEGA ERM

Eine Bewertungsvorlage dient als Vorlage zur Erstellung von Bewertungskampagnen und -sitzungen. Die Bewertungsvorlage legt den Umfang der Bewertung fest, sowie die zu verwendende Fragebogenvorlage und eventuell die Aggregationsschemen, die für die Auslegung der globalen Ergebnisse verwendet werden.

Übersicht über die verschiedenen angebotenen Modelle

Mit diesen Bewertungsvorlagen in **MEGA ERM** soll eine Bewertung der Risiken bei einer Entität oder einem Prozess erhalten werden.

Die Bewertung bezieht sich entweder nur auf Risiken oder auf die Risiken und Kontrollen dieser Risiken.

In der folgenden Tabelle wird das Modell angegeben, das abhängig vom Bedarf verwendet wird.

Bewertung	nur von Risiken	von Risiken, die durch Kontrollen gemindert werden
Nach Entität	- Bewertung nur von Risiken - nach Entität	- Bewertung der Risiken - nach Entität - Bewertung der Kontrollen - nach Entität
Nach Prozess	- Bewertung nur von Risiken - nach Entität, nach Prozess	- Bewertung der Risiken - nach Entität, nach Prozess - Bewertung der Kontrollen - nach Entität, nach Prozess

Um die in **MEGA ERM** angebotenen Bewertungsvorlagen zu beschreiben, müssen folgende Elemente verwendet werden:

- Die bewerteten Merkmale
- Die bewerteten Objekte
- Der Kontext der Objektbewertung
- Die Beantworter
- Die Fragebögen
- Das Aggregationsschema

Die bewerteten Merkmale

Ein bewertetes Merkmal legt fest, was bei einer Bewertung bewertet werden soll. Das Merkmal kann mit einer MetaClass verbunden werden, vor allem mit einem der MetaAttributs, zum Beispiel. Metaclasse Risiko, MetaAttribut: Wahrscheinlichkeit.

Bewertung	nur von Risiken	von Risiken, die durch Kontrollen gemindert werden
Nach Entität Nach Prozess	- Auswirkung - Wahrscheinlichkeit - Bruttorisiko - Design der Kontrollen - Wirksamkeit der Kontrollen - Kontrollebene	Für die Risiken - Auswirkung - Wahrscheinlichkeit - Bruttorisiko - Nettorisiko Für die Kontrollen - Design der Kontrolle - Kontrollwirksamkeit - Kontrollebene

Die bewerteten Objekte

Die Objekte sind Risiken und Kontrollen.

- Die Liste der Risiken wird abhängig des Bewertungsgegenstands erstellt: Entität oder Prozess.
- Die Liste der Kontrollen wird von der Liste der Risiken abgeleitet

<table>
<tr><th>Bewertung</th><th>nur von Risiken</th><th>von Risiken, die durch Kontrollen gemindert werden</th></tr>
<tr><td rowspan="2">Nach Entität</td><td colspan="2">Die Liste der zu bewertenden Risiken setzt sich aus allen Risiken bei der Entität (Objekt der Bewertung) und ihren Unterentitäten zusammen</td></tr>
<tr><td></td><td>Die Liste der zu bewertenden Kontrollen setzt sich aus den Kontrollen der zu bewertenden Risiken zusammen</td></tr>
<tr><td rowspan="2">Nach Prozess</td><td colspan="2">Die Liste der zu bewertenden Risiken setzt sich aus allen Risiken beim Prozess (Objekt der Bewertung) und seinen Unterprozessen zusammen</td></tr>
<tr><td></td><td>Die Liste der zu bewertenden Kontrollen setzt sich aus den Kontrollen der zu bewertenden Risiken zusammen</td></tr>
</table>

Der Bewertungskontext

Der Bewertungskontext wird mit dem Umfang der zu bewertenden Risiken beschrieben. Bei den Bewertungsvorlagen in **MEGA ERM** wird dieser Umfang mit den Entitäten und Prozessen beschrieben, die für die Sitzung als Parameter angegeben wurden.

Die Beantworter

Bei den Bewertungsvorlagen in **MEGA ERM** sind Beantworter Personen, die für die Entität als **Risikobewerter** definiert wurden.

☛ *Weitere Informationen zu den Merkmalen der Entitäten einer Organisation finden Sie unter "Organisation definieren", Seite 26.*

Die Fragebögen

In einem Fragebogen wird eine Liste von vordefinierten Fragen aufgeführt, die für einen Ereignistyp, eine Kontrolle, ein Dokument usw. gelten können.

☛ *Weitere Informationen zu den Fragebogenvorlagen finden Sie unter "Die Fragebogenvorlagen", Seite 56.*

Die Fragebögen beziehen sich auf die zu bewertenden Merkmale aller Risiken oder Kontrollen, die als Objekt der Bewertung festgelegt wurden.

Bewertung	nur von Risiken	von Risiken, die durch Kontrollen gemindert werden
Nach Entität Nach Prozess	- Auswirkung - Wahrscheinlichkeit - Design der Kontrollen - Wirksamkeit der Kontrollen	Für die Risiken - Auswirkung - Wahrscheinlichkeit Für die Kontrollen - Design der Kontrolle - Kontrollwirksamkeit

Das Aggregationsschema

Mit den Bewertungsvorlagen in **MEGA ERM** stützt sich jeder angegebene Bewertungswert auf einen "Bewertungsknoten", der den für ein Merkmal eines Objekts (Risiko oder Kontrolle) angegebenen Wert in einem genauen Kontext beschreibt, der mit einer Entität, einem Beantworter und eventuell einem Prozess definiert wurde.

Die "Bewertungsknoten" können als Baumstruktur bis zum Stammknoten dargestellt werden. Der Stammknoten kann sein:

- ein Risiko
- eine Entität
- ein Prozess
- ein Risikotyp

Jeder "Aggregationsknoten" bezieht sich auf die Werte der Maße, die in den bewerteten Merkmalen definiert wurden. Mit den Ergebnissen der Aggregation dieser Werte können Aggregationsberichte erhalten werden.



1. Aggregation - Risk Level per Process

	ERM Avg Impact	ERM Avg Inherent Risk	ERM Avg Likelihood	ERM Impact	ERM Inherent Risk	ERM Likelihood
Operations	Very Low	Low	Probable			
R&D						
Counterparty risks				High	High	Probable
Natural catastrophy						
Fraud & Corruption				Very Low	Low	Probable
Security leaks				Very Low	Low	Possible
Work accidents				Very Low	Very Low	Rare

Ein Aggregationsschema ist eine Reihe von Schritten, mit denen die Ergebnisse einer Bewertung nach festgelegten Bewertungsregeln konsolidiert werden.

Die Aggregationsschemen der Bewertungsvorlagen in **MEGA ERM** definieren den Berechnungsmodus:

- der Bruttowerte der einzelnen Risiken
  Im Beispiel des Aggregationsberichts, handelt es sich bei den dargestellten Werten um: die Auswirkung, die Wahrscheinlichkeit und das inhärente Risiko.
- der berechneten Werte (maximaler und durchschnittlicher Wert) der Entitäten, Prozesse und Risikotypen.
  Im Beispiel des Aggregationsberichts, handelt es sich bei den dargestellten Werten um: die berechneten durchschnittlichen Werte bei allen Risiken eines Prozesses in Bezug auf die Auswirkung, die Wahrscheinlichkeit und das inhärente Risiko.

Das Prinzip der Rechenregeln, die bei den Bewertungsvorlagen in **MEGA ERM** verwendet werden, wird in der folgenden Tabelle beschrieben.

<table>
<tr><th>Bewertung</th><th>nur von Risiken</th><th>von Risiken, die durch Kontrollen gemindert werden</th></tr>
<tr><td rowspan="2">Nach Entität</td><td colspan="2">Die Werte sind mit dem Risiko ’Ri’ verbunden und werden ab den Werten berechnet, die für dieses Risiko bei jeder betroffenen Einheit ’Ej’ angegeben wurden. Die berücksichtigten Bewertungsknoten, die mit den Paaren (Ri, Ej) verbunden sind
- Auswirkung von Ri = Max. und Durchschn. {Auswirkung der (Ri, Ej) für alle j}
- Wahrscheinlichkeit von Ri = Max. und Durchschn. {Wahrscheinlichkeit der (Ri, Ej) für alle j}
- Bruttorisiko von Ri = Max. und Durchschn. {Bruttorisiko der (Ri, Ej) für alle j}
- Design der Kontrollen von Ri = Max. und Durchschn. {Design der Kontrollen der (Ri, Ej) für alle j}
- Wirksamkeit der Kontrollen von Ri = Max. und Durchschn. {Wirksamkeit der Kontrollen der (Ri, Ej) für alle j}
- Kontrollebene von Ri = Max. und Durchschn. {Kontrollebene der (Ri, Ej) für alle j}</td></tr>
<tr><td></td><td>Die Minderungswerte bei jedem Bewertungsknoten (Ri, Ej) werden mit dem Durchschnittswert der Werte erhalten, die für die Kontrollen Ck angegeben wurden, welche mit dem Risiko Ri verbunden sind.
- Design der Kontrollen von (Ri, Ej) = Max. und Durchschn. {Design der Kontrollen (Ri, Ej, Ck) bei allen k}
- Wirksamkeit der Kontrollen von (Ri, Ej) = Max. und Durchschn. {Wirksamkeit der Kontrollen (Ri, Ej, Ck) bei allen k}
- Kontrollebene von (Ri, Ej) = Max. und Durchschn. {Kontrollebene (Ri, Ej, Ck) bei allen k}</td></tr>
<tr><td rowspan="2">Nach Prozess</td><td colspan="2">Die Werte sind mit dem Risiko ’Ri’ verbunden und werden ab den Werten berechnet, die für dieses Risiko bei jedem betroffenen Prozess ’Pj’ angegeben wurden. Die berücksichtigten Bewertungsknoten, die mit den Paaren (Ri, Pj) verbunden sind
- Auswirkung von Ri = Max. und Durchschn. {Auswirkung der (Ri, Pj) für alle j}
- Wahrscheinlichkeit von Ri = Max. und Durchschn. {Wahrscheinlichkeit der (Ri, Pj) für alle j}
- Bruttorisiko von Ri = Max. und Durchschn. {Bruttorisiko der (Ri, Pj) für alle j}</td></tr>
<tr><td></td><td>Die Kontrollwerte bei jedem Bewertungsknoten (Ri, Pj) werden mit dem Durchschnittswert der Werte erhalten, die für die Kontrollen Ck angegeben wurden, welche mit dem Risiko Ri verbunden sind.</td></tr>
</table>

Bewertungssitzung verwalten

Für den Versand von Bewertungsfragebögen wird eine *Bewertungssitzung* erstellt.

Eine Bewertungssitzung ist eine Bewertung, die zu einem bestimmten Zeitpunkt gestartet wird. Mit der Veröffentlichung der Bewertungssitzung soll ein Bewertungsfragebogen gesendet werden, in dem die Fragen gezielt an die Bewerter gerichtet werden.

Übersicht über die einzelnen Schritte einer Bewertung mit einem Fragebogen

Im Folgenden finden Sie eine Übersicht über die Schritte, die für den Start einer Bewertungskampagne durchgeführt werden müssen:

1. Sicherstellen, dass die notwendigen Objekte für den Start der Bewertungssitzungen existieren: Lenkungskalender, Bewertungsvorlagen und Fragebögen.
2. Eine *Bewertungskampagne* erstellen und den Umfang dieser Kampagne definieren

   In einer Kampagne können mehrere Bewertungssitzungen gruppiert werden.
3. Eine *Bewertungssitzung* erstellen.
4. Die Bewertungssitzung starten.
   Bewertungsfragebögen werden an die entsprechenden Benutzer nach dem gewählten Bereitstellungsmodus gesendet.

   In einem Fragebogen wird eine Liste von vordefinierten Fragen aufgeführt, die für einen Ereignistyp, eine Kontrolle, ein Dokument usw. gelten können.
5. Die Ergebnisse der Bewertungskampagne analysieren.

   Weitere Informationen zu den Schritten der Bearbeitung einer Bewertungssitzung finden Sie unter "Workflow einer Bewertungssitzung", Seite 112.

Bewertungskampagne erstellen

In einer Kampagne können mehrere Bewertungssitzungen gruppiert werden.

Um eine *Kampagne* zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Risiko > Kampagnenmanagement > Leitung der Kampagnen > Ausführung > Kampagnen**.
   Die Liste der Kampagnen wird in der Bearbeitungszone angezeigt.
2. Klicken Sie auf **Neu**.
   Daraufhin wird das Fenster zum Erstellen einer Kampagne geöffnet.

3. Geben sie auf der Seite Folgendes an:
   - den **Eigentümer der Kampagne**
   - die **Bewertungsvorlage**
   - einen **Kampagnenkalender**

     ☛ *Ein Kalender besteht aus Kalenderperioden, die zum Erstellen des Kampagnenumfangs notwendig sind. Dieser Kalender muss also verwendet werden, wenn Sie einen Kampagnenumfang für die Selbstbewertung der Kontrollen festlegen möchten.*
   - ein **Anfangsdatum**
   - ein **Enddatum**
4. Klicken Sie auf die Schaltfläche **Weiter**.
5. Wählen Sie den Namen der Entität (oder des Prozesses, je nach verwendeter Bewertungsvorlage) aus, ab der die Liste der Risiken erstellt werden soll.
6. Klicken Sie auf die Schaltfläche **Bericht auffrischen**.
   In dem geöffneten Bericht kann der berechnete Umfang für die Kampagne angezeigt werden.

   ☛ *Auf dieses Fenster, mit der Liste der Parameter der Bewertungskampagne, kann weiterhin in der Registerkarte **Vorschau und Parameter** des Eigenschaftsfensters einer Bewertungskampagne zugegriffen werden.*

   ☛ *Ausführliche Informationen zu diesem Bericht finden Sie unter "Vorschau der Sitzung vor dem Start", Seite 64.*
7. Klicken Sie auf **OK**.

Bewertungssitzung erstellen

Ab der erstellten Kampagne erstellen Sie nun eine Bewertungssitzung.

📖 *In einer Kampagne können mehrere Bewertungssitzungen gruppiert werden.*

U m eine *Bewertungssitzung* ab einer Kampagne zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie das Eigenschaftsfenster der Kampagne und klicken Sie auf die Registerkarte **Sitzungen**.
   Im oberen Bereich der Bearbeitungszone wird ein Bericht über die Planung der aktuellen Sitzungen angezeigt.
2. Klicken Sie im Abschnitt **Bewertungssitzung** auf **Neu**.
   Die neue Sitzung wird in der Liste der Kampagnensitzungen aufgeführt.
3. Öffnen Sie das Eigenschaftsfenster der neuen Sitzung und klicken Sie auf die Registerkarte **Merkmale**.
4. Geben Sie den **Namen** der Sitzung an.
5. Der **Durchführungsverantwortliche der Sitzung** wird mit dem Namen des Benutzers initialisiert, der die Sitzung erstellt hat. Dieser Wert kann aber geändert werden.
6. Wählen Sie eine Fragebogenvorlage aus.
7. Das **für den Beginn der Bewertung geplante Datum** wird auf das aktuelle Datum festgelegt.
8. Das **für das Ende der Bewertung geplante Datum** wird auf das Enddatum der Kampagne festgelegt.
9. Wählen Sie die Registerkarte **Vorschau und Parameter** aus.

10. Wählen Sie eventuell den Namen eines anderen Bewertungsparameters (Entität oder Prozess, je nach verwendeter Bewertungsvorlage) aus, ab dem die Liste der Risiken erstellt werden soll.
11. Klicken Sie auf die Schaltfläche **Bericht auffrischen**.
    In dem geöffneten Bericht kann der berechnete Umfang für die Sitzung angezeigt werden.

    ☛ *Ausführliche Informationen zu diesem Bericht finden Sie unter* *"Vorschau der Sitzung vor dem Start", Seite 64.*
12. Klicken Sie auf **OK**.

Bereitstellung einer Bewertungssitzung vorbereiten

Bei der Bereitstellung einer Bewertungssitzung wird der Versand der Fragebögen an die Benutzer vorbereitet, die als Beantworter der zu bewertenden Risiken definiert wurden.

Vorschau der Sitzung vor dem Start

Vor dem Start der Sitzung wird eine Zusammenfassung über diese Sitzung als Bericht generiert.

Um die Vorschau des Sitzungsberichts anzuzeigen, gehen Sie wie folgt vor:

- Öffnen Sie das Eigenschaftsfenster der Bewertungssitzung und klicken Sie auf die Registerkarte **Vorschau und Parameter**.
  Im Bericht werden aufgeführt:
  - die Kampagne
  - die Sitzung, das Anfangs- und das Enddatum
  - die Liste der bewerteten Merkmale
  - die Liste der zu bewertenden Objekte
  - die Liste der Elemente im Bewertungskontext (Entitäten und Prozesse)
  - die Liste der Beantworter
  - die Liste der Bewertungsknoten

Eine Bewertungssitzung bereitstellen

Mit einem Befehl können Sie alle Bewertungsknoten für die Sitzung berechnen. Anschließend kann der Verantwortliche der Sitzung die Liste dieser Knoten überarbeiten und Knoten entfernen oder bestimmte Parameter ändern.

Um die Liste der Bewertungsknoten einer Sitzung zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie das Eigenschaftsfenster der Kampagne und klicken Sie auf die Registerkarte **Sitzung**.
2. Klicken Sie im Abschnitt **Bewertungssitzung** mit der rechten Maustaste auf die betroffene Sitzung und wählen Sie den Befehl **Bereitstellen** aus.
   Dieser Vorgang kann einige Minuten in Anspruch nehmen.

Um auf die Liste der berechneten Bewertungsknoten zuzugreifen, gehen Sie wie folgt vor:

- Öffnen Sie das Eigenschaftsfenster der Bewertungssitzung und klicken Sie auf die Registerkarte **Effektiver Umfang**.
  Nun wird die Liste der berechneten Knoten angezeigt.

In dieser Liste können Sie:

- Knoten löschen
- den für einen Knoten festgelegten Beantworter ändern

Bewertungssitzung freigeben

Bei diesem Schritt können Sie die Fragebögen generieren, ohne sie an die Empfänger zu senden.

In einem Fragebogen wird eine Liste von vordefinierten Fragen aufgeführt, die für einen Ereignistyp, eine Kontrolle, ein Dokument usw. gelten können.

Um eine Bewertungssitzung freizugeben, gehen Sie wie folgt vor:

1. Öffnen Sie das Eigenschaftsfenster der Kampagne und klicken Sie auf die Registerkarte **Sitzung**.
2. Klicken Sie im Abschnitt **Bewertungssitzung** mit der rechten Maustaste auf die betroffene Sitzung und wählen Sie den Befehl **Freigeben** aus.
   Alle Fragebögen werden mit dem Status "Zu senden" erstellt. Dieser Vorgang kann einige Minuten in Anspruch nehmen.

Um auf die Liste der generierten Fragebögen zuzugreifen, gehen Sie wie folgt vor:

1. Öffnen Sie das Eigenschaftsfenster der Sitzung und klicken Sie auf die Registerkarte **Fragebögen**.
   Nun erscheint eine Liste der Beantworter.
2. Wählen Sie einen Beantworter aus und klicken Sie auf die Schaltfläche **Fragebögen anzeigen**.
   Im Fenster wird die Liste der Fragen angezeigt, die an den Beantworter gesendet werden.

In einem Fragebogen wird eine Liste von vordefinierten Fragen aufgeführt, die für einen Ereignistyp, eine Kontrolle, ein Dokument usw. gelten können.

Bewertungssitzung starten

Um die Sitzung zu starten, gehen Sie wie folgt vor:

1. Klicken Sie auf **Risiko > Kampagnenmanagement > Leitung der Kampagnen > Ausführung > Kampagnen**.
   Die Liste der Kampagnen wird in der Bearbeitungszone angezeigt.
2. Wählen Sie die Kampagne in der Liste aus und öffnen Sie das Eigenschaftsfenster der Kampagne.
3. Klicken Sie im Abschnitt **Sitzung** mit der rechten Maustaste auf die betroffene Sitzung und wählen Sie den Befehl **Aktivieren** aus.
   Daraufhin wird das Fenster zum Aktivieren der Sitzung geöffnet.

4. Klicken Sie auf **OK**.
   Die *Bewertungsfragebögen* werden an die Empfänger gesendet.

Sie können die Sitzung ggf. jederzeit abbrechen.

Fortschritt der Sitzung verfolgen

Ergebnis der Sitzung aufrufen

Um den Fortschritt einer Bewertungssitzung aufzurufen, gehen Sie wie folgt vor:

- Öffnen Sie die Eigenschaftsseite der Bewertungssitzung und klicken Sie auf die Registerkarte **Bericht**.

Bewertungsfragebögen freigeben

Um auf die Liste der Fragebögen zuzugreifen, die von den Beantwortern ausgefüllt wurden, gehen Sie wie folgt vor:

1. Klicken Sie auf **Risiko > Home > Mein Desktop > Meine Verantwortungsbereiche>Meine Bewertungsfragebögen**.
   Die Liste der ausgefüllten Fragebögen wird angezeigt. Der Status des Workflows hat nun den Wert "Freizugeben" angenommen.
2. Wählen Sie den betroffenen Fragebogen aus und klicken Sie auf die Schaltfläche **Fragebögen anzeigen**.
   Der Inhalt des Fragebogens wird in einer neuen Registerkarte angezeigt.

Sie können:

- die Antworten **freigeben**, wenn der Fragebogen Ihrer Meinung nach richtig ausgefüllt wurde.
  Der Fragebogen wird geschlossen und die Ergebnisse werden automatisch berechnet.
- für den Fragebogen die **Überarbeitung beantragen**.
  Der Beantworter erhält eine Nachricht mit der Mitteilung, dass er den Fragebogen erneut ausfüllen muss.

Erstellung eines Aktionsplans hervorrufen

Wenn sich aus den Antworten eines Fragebogens ergibt, dass der Wert **Nettorisiko** für ein in einem bestimmten Kontext bewertetes Risiko **Erhöht** oder **Sehr hoch** ist, wird automatisch ein Aktionsplan mit folgenden Merkmalen erstellt:

- **Name**: "Proposed action plan for Risk Rx"
- **Eigentümer**: Eigentümer des bewerteten Risikos.
- **Kommentare**: wird automatisch mit folgenden Informationen eingegeben:
  - Datum
  - Name der Kampagne und der Sitzung
  - Name des Beantworters
  - Name der Entität, die den Kontext definiert
  - Name des Prozesses, der den Kontext definiert
- Der Abschnitt **Umfang** wird automatisch mit den Elementen aktualisiert, die den Bewertungskontext definieren: Prozesse und Entitäten.

  ☛ *Weitere Informationen zu den Aktionsplänen finden Sie unter* *"Aktionsplan erstellen", Seite 73*.

Bewertungssitzung schließen

Sie können die Sitzung jederzeit schließen, auch wenn die Fragebögen von den Beantwortern nicht ausgefüllt wurden.

Um eine Bewertungssitzung zu schließen, gehen Sie wie folgt vor:

1. Öffnen Sie das Eigenschaftsfenster der Kampagne und klicken Sie auf die Registerkarte **Sitzung**.
2. Klicken Sie im Abschnitt **Bewertungssitzung** mit der rechten Maustaste auf die betroffene Sitzung und wählen Sie den Befehl **Schließen** aus.
   Alle Sitzungen werden automatisch geschlossen. Dieser Vorgang kann einige Minuten in Anspruch nehmen.

Fragebögen ausfüllen

Die hier beschriebenen Schritte betreffen die Beantworter.

☛ *Weitere Informationen zu den Schritten der Bearbeitung eines Fragebogens finden Sie unter "Workflow eines Fragebogen", Seite 114.*

Zugriff auf Bewertungsfragebögen

Nach dem Start einer Bewertungssitzung erhalten die Empfänger des Fragebogens eine Benachrichtigung.

Um auf die Liste der Bewertungsfragebögen zuzugreifen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Home > Home Fragebögen > Meine Bewertungsfragebögen**.
   Die Liste der auszufüllenden Fragebögen wird angezeigt.
2. Wählen Sie den betroffenen Fragebogen aus und klicken Sie auf die Schaltfläche **Fragebögen anzeigen**.
   Der Inhalt des Fragebogens wird in einer neuen Registerkarte angezeigt.

Fragebogen bearbeiten

Wenn er den Inhalt eines Fragebogens aufgerufen hat, kann der Beantworter:

- den Fragebogen **schließen**, ohne ihn zu beantworten.
- die **Übertragung des Fragebogens** an einen anderen Beantworter anfordern

  ☛ *In diesem Fall wird der Verantwortliche der Sitzung per E-Mail benachrichtigt. Er muss einen anderen Beantworter wählen.*
- die Antwort im Fragebogen an eine andere Person **delegieren**.

  ☛ *In diesem Fall wird die ausgewählte Person per E-Mail benachrichtigt.*
- Den Fragebogen akzeptieren und beantworten

Fragen beantworten

Wenn Sie die entsprechenden Kästchen markiert haben, hat der Beantworter mehrere Möglichkeiten:

- **Speichern**: Um die Antworten zu speichern, ohne sie sofort zu senden. So kann der Fragebogen auch später ergänzt werden.
- Die Antwort zur Freigabe durch den Verantwortlichen der Sitzung **einreichen**.

5

RISIKEN BEARBEITEN

Besonders wichtig ist es, die Ursachen der Risiken zu identifizieren, damit diese Risiken, und nicht nur ihre Symptome bearbeitet werden. Durch die Bewertung der Risiken wurden Elemente eingebracht, mit denen die besten Strategien einer Bearbeitung mit dem besten Kosten/ Leistungsverhältnis gewählt werden können.

In **MEGA ERM** können Sie festgelegte Aktionspläne angeben, umsetzen und verfolgen, um Risiken zu bearbeiten.

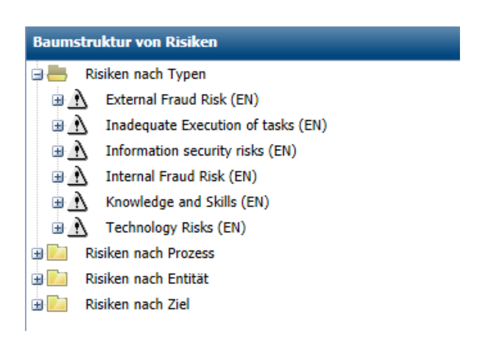
In diesem Kapitel werden folgende Punkte behandelt:

BESCHREIBEN, WIE EIN RISIKO BEARBEITET WIRD

Modus der Risikobearbeitung

Um die Wahl der Bearbeitungen eines Risikos anzugeben, gehen Sie wie folgt vor:

- Öffnen Sie das Eigenschaftsfenster des Risikos und klicken Sie auf die Registerkarte **Bearbeitung**.



Bearbeitungsmodi

Zum Bearbeiten von Risiken stehen mehrere Lösungen zur Verfügung.

- ***Akzeptanz***
  Die Strategie im Risikomanagement, mit einer fundierten Entscheidung, das Risiko zu akzeptieren. Solange nicht die Absicht gezeigt wird, das Risiko zu bearbeiten, kann die Organisation mit dieser Strategie nicht gegen das Risiko geschützt werden.
- ***Reduzierung***
  Die Häufigkeit des Risikos kann reduziert werden, wenn weitere Kontrollen eingerichtet oder die Auswirkung der Folgen reduziert wird, sollte dieses Risiko auftreten.
- ***Verlagern*** (Zulieferer)
  Das Risiko kann auch mit anderen Partnern geteilt werden, vor allem, wenn die Partner kompetenter sind, um das Risiko unter Kontrolle zu halten. So kann beispielsweise eine gefährliche Aktivität an einen auf den betreffenden Bereich spezialisierten Partner übertragen werden. In diesem Fall muss oftmals eine neue Untersuchung über die Risiken durchgeführt werden, da die Einführung eines neuen Partners weitere Risiken mit sich bringen können.
- ***Versicherung***
  Abgesehen von den oben erwähnten Ansätzen muss oftmals eine Versicherung abgeschlossen werden, vor allem für Risiken, die nicht häufig auftreten, aber hohe Auswirkungen haben. In diesem Fall verlangt

die Versicherung im Allgemeinen, Präventionsmaßnahmen zur Risikominderung zu ergreifen.

Die möglichen verschiedenen Szenarios werden später analysiert. Dabei werden die positiven und negativen Aspekte verglichen, um ein Szenario zu erhalten, das sich mit der gewünschten Ebene der Risikokontrolle vereinbaren lässt.

Je nach gewählter Lösung müssen ihre Folgen in Bezug auf die Häufigkeit und die Auswirkung sowie die Kosten und Nutzen berücksichtigt werden.

Mit einem Kommentar können Sie den Modus der Risikobearbeitung angeben.

Bei der Bearbeitung muss eine Lösung gewählt werden, mit der das **Restrisiko** unter den von der Geschäftsleitung gewünschten Toleranzwert sinkt.

Im Feld **Ziel-Risiko** können Sie die Höhe des Risikos angeben, die von der Organisation akzeptiert wird.

Umzusetzende Aktionen angeben

Das Management arbeitet mehrere Aktionen aus, um die Höhe der Risiken mit dem Toleranzgrenzwert und dem Risiko-Appetit des Unternehmens abzustimmen.

Bei jedem Risiko wird das gewählte Szenario ausführlich beschrieben. Dabei werden die verschiedenen Risikofaktoren und eingesetzten Kontrollen beschrieben. Zudem wird angegeben, welche Kontrollen eingerichtet werden, um das Risiko zu verhindern, und welche kurativen Abläufe durchgeführt werden, sollte das Risiko auftreten.

Bei einer Verlagerung des Risikos auf einen Partner oder eine Versicherung werden die Verträge angegeben, die zwischen den Parteien abgeschlossen werden müssen. Auch die voraussehbare Auswirkung auf die Prozesse innerhalb des Unternehmens wird aufgeführt.

Präventive Kontrollen zur Reduzierung der Häufigkeit und der Auswirkung des Risikos können eine Lösung für die Risikominderung sein.

Um die Kontrolle(n) und Aktionspläne für die Risikoverhütung anzugeben, gehen Sie wie folgt vor:

- Klappen Sie auf der Eigenschaftsseite eines Risikos in der Registerkarte **Bearbeitung** den Abschnitt **Kontrollen und Aktionspläne** auf.
  - In der Registerkarte **Aktionsplan** wird die Liste der eingerichteten Aktionspläne aufgeführt: Zum Beispiel zum Erstellen oder Verbessern einer Kontrolle, für das Krisenmanagement bei einem Zwischenfall oder für einen vollkommen überarbeiteten Prozess, um ihn zu verbessern.

    Ein Aktionsplan besteht aus einer Reihe von Aktionen. Der Aktionsplan soll die Risiken oder Ereignisse reduzieren, die sich auf die Aktivitäten des Unternehmens negativ auswirken bzw. die Effizienz eines Prozesses oder einer Organisation verbessern können.
  - In der Registerkarte **Kontrolle** wird die Liste der Kontrollen aufgeführt, die zur Reduzierung des Risikos geplant wurden.

    Eine Kontrolle ist ein Mittel, ein oder mehrere Risiken unter Kontrolle zu haben, und sicherzustellen, dass eine gesetzliche,

vorschriftsmäßige oder interne Anforderung des Unternehmens erfüllt wird.

AKTIONSPLAN BEANTRAGEN

Ein *Aktionsplan* kann eingerichtet werden, zum Beispiel zum Erstellen oder Verbessern einer Kontrolle, für das Krisenmanagement bei einem Zwischenfall oder für einen vollkommen überarbeiteten Prozess, um ihn zu verbessern.

Ein Aktionsplan besteht aus einer Reihe von Aktionen. Der Aktionsplan soll die Risiken oder Ereignisse reduzieren, die sich auf die Aktivitäten des Unternehmens negativ auswirken bzw. die Effizienz eines Prozesses oder einer Organisation verbessern können.

Der Aktionsplan wird entweder separat erstellt und mit verschiedenen Objekten verbunden (Risiken, Prozesse, Kontrollen, Entitäten usw.) oder direkt ab einem dieser Objekte erstellt.

Aktionsplan erstellen

Um einen Aktionsplan ab einem Risiko zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie die Eigenschaftsseite eines Risikos und klicken Sie auf die Registerkarte **Bearbeitung**.
2. Klappen Sie den Abschnitt **Kontrollen und Aktionspläne** auf und klicken Sie auf die Registerkarte **Aktionsplan**.
3. Klicken Sie auf die Schaltfläche **Neu**.
   Der neue Aktionsplan wird in der Liste der Aktionspläne des Risikos erstellt. Der Aktionsplan wird mit dem Status "Geöffnet" erstellt.

☛ *Sie können die weiteren Felder später ausfüllen.*

Aktionsplan charakterisieren

Bevor der Aktionsplan zur Zustimmung vorgelegt wird, kann der Antragsteller weitere Informationen im Aktionsplan angeben.

Um die Felder zu aktualisieren, die einen Aktionsplan charakterisieren, gehen Sie wie folgt vor:

1. Klicken Sie auf **Home > Mein Desktop > Meine Verantwortungsbereiche>Meine Aktionspläne**.
2. Wählen Sie auf der nun geöffneten Seite den betroffenen Aktionsplan aus und klicken Sie auf **Eigenschaften**.

Allgemeine Merkmale

Im Abschnitt **Merkmale** können Sie die Felder des Aktionsplans ausfüllen, zum Beispiel:

- **Name**: Name des Aktionsplans
- **Eigentümer**: Dieses Feld wird standardmäßig von dem Benutzer ausgefüllt, der den Aktionsplan erstellt.
- **Entitätseigentümer**: Ermöglicht, die Liste der Benutzer als Eigentümer einzugrenzen.
- **Freigabeverantwortlicher**: Benutzer, der für die Freigabe des Aktionsplans verantwortlich ist, wenn alle Aktionen abgeschlossen sind.
- **Mittel**: Text als Beschreibung der notwendigen/gewünschten Mittel für die Ausführung des Aktionsplans.
- **Priorität**: um eine Stufe anzugeben. Die Priorität kann verschiedene Stufen haben: "niedrig", "mittel", "hoch" oder "kritisch".
- **Organisatorischer Level**: endgültiges Ziel des Plans; "Global" oder "Lokal".
- **Ursprung**: ermöglicht, den Kontext der Durchführung eines Aktionsplans festzulegen : "Audit", "Konformität", "Ereignis", "Risiko", "RFC" oder "Sonstiges".
- **Kategorie**: um die eingeleitete Aktion anzugeben, wie zum Beispiel: "Verbesserung der Prozesse".
- **Art**: um die Art des eingeleiteten Aktionsplans zu definieren: "Präventiv" oder "Korrektiv".
- **Kommentare**: ermöglicht, weitere Informationen zum Aktionsplan und zu seinen Merkmalen anzugeben.

RACI

Der Benutzer, der für den Aktionsplan als **Durchführungsverantwortlicher** definiert wurde, ist für die Festlegung der durchzuführenden Aktionen und für ihre Durchführung verantwortlich. Dieses Feld wird von dem Benutzer ausgefüllt, der den Aktionsplan erstellt, oder vom Freigabeverantwortlichen des Aktionsplans.

☛ *Weitere Informationen zur Verwendung von RACI finden Sie im Handbuch **HOPEX Solutions Common Features**.*

Finanzanalyse

- **Geplante Kosten**: geschätzte Kosten des Aktionsplans, die in der **Währung** ausgedrückt werden.
- **Reelle Kosten**: reelle Kosten des Aktionsplans, die in der **Währung** ausgedrückt werden.
- **Geplante Kosten (Tage/Mann)**: geschätzte Arbeitslast, die in Tagen/Mann ausgedrückt wird und für die Umsetzung des Aktionsplans notwendig sind.
- **Reelle Kosten (Tag-Mann)**: geschätzte Arbeitslast in Tagen/Mann für die Umsetzung des Aktionsplans.

Erfolgsfaktoren

Im Abschnitt **Schlüsselfaktor für den Erfolg** können Sie Erfolgsindikatoren als Text eingeben, mit denen der Erfolg des Aktionsplans beurteilt werden kann.

- **Schlüsselfaktoren für den Erfolg**: Textinformationen zu den Erfolgsfaktoren des Aktionsplans.
- **Erfolg**: Informationen zum endgültigen Erfolg des Aktionsplans: "Keiner", "Erfolg" oder "Misserfolg"
- **Kommentare zum Erfolg**: Textinformationen zu den Ergebnissen des Aktionsplans.

Umfang

Um einen Aktionsplan in seiner Umgebung zu positionieren, können Sie im Abschnitt **Umfang** mit dem Aktionsplan Objekte verbinden.

Sie können Objekte wie Risiken, Geschäftsprozesse und organisatorische Prozesse, Kontrollen, Entitäten oder Anwendungen verbinden.

Meilensteine

Meilensteine sind wichtige Daten des Aktionsplans. Sie können diese Daten auch später angeben.

- **Effektives Anfangsdatum** und **Geplantes Anfangsdatum**,
- **Effektives Enddatum** und **Geplantes Enddatum**,

Anlagen

Sie können Geschäftsdokumente als Anlage an einen Aktionsplan anhängen.

☛ *Weitere Informationen zur Verwendung von Geschäftsdokumenten finden Sie im Handbuch* ***HOPEX Solutions Common Features****.*

Fortschrittsverfolgung des Aktionsplans vorbereiten

Der Verantwortliche des Aktionsplans kann den Fortschritt eines Aktionsplans regelmäßig in Prozenten angeben.

☛ *Weitere Informationen zur Erstellung eines Lenkungsdatums finden Sie unter* *"Fortschrittsstatus eines Aktionsplans angeben", Seite 77**.*

MEGA ERM bietet die Möglichkeit, den Verantwortlichen des Aktionsplans regelmäßig aufzufordern, den Fortschritt des Plans anhand eines Lenkungskalenders anzugeben.

Lenkungskalender

Sie können mit dem Aktionsplan einen **Lenkungskalender** verbinden, damit regelmäßig eine Nachricht an den Verantwortlichen des Aktionsplans gesendet wird, damit er den Fortschritt dieses Plans angibt.

Mit dem Lenkungskalender können wiederholte Aktionen zu vordefinierten Terminen durchgeführt werden. Man kann den Kalender zum Beispiel verwenden, um Erinnerungen an die Person zu senden, die für einen Aktionsplan verantwortlich ist, damit sie den Fortschritt

angibt, der bei diesem Aktionsplan erzielt wurde. Man kann einen Lenkungskalender auch verwenden, um den Start von Bewertungssitzungen zu regelmäßigen Terminen auszulösen ...

Um einen Lenkungskalender für einen Aktionsplan zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie die Eigenschaftsseite des Aktionsplans.
2. Klicken Sie im Abschnitt **Merkmale** auf den Pfeil rechts neben dem Feld **Lenkungskalender**.
   Nun erscheint eine Liste der verfügbaren Befehle.
3. Wählen Sie **Erstellen** aus.
   Daraufhin wird die Seite zum Erstellen eines Lenkungskalenders angezeigt.
4. Geben Sie den **Namen** des Lenkungskalenders an.
5. Der **Typ des Lenkungskalenders** wird automatisch angegeben.
6. Klicken Sie im Abschnitt **Lenkungsdaten** auf **Verbinden**.
7. Wählen Sie die betreffenden Lenkungsdaten aus.

   ☛ *Weitere Informationen zur Erstellung eines Lenkungsdatums finden Sie unter* *"Lenkungsdatum erstellen", Seite 76**.*

8. Klicken Sie auf **OK**.

Lenkungsdatum erstellen

Ein Lenkungsdatum ist ein Datum, das in einem Lenkungskalender festgelegt wird und an dem der verantwortlichen Person eines Elements eine Erinnerung gesendet wird. Ein Anfangsdatum, ein Erinnerungsdatum oder ein Termin (Enddatum).

Um ein Lenkungsdatum für einen existierenden Lenkungskalender zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie die Eigenschaftsseite des Aktionsplans.
2. Klicken Sie im Abschnitt **Merkmale** auf den Pfeil rechts neben dem Feld **Lenkungskalender**.
   Nun erscheint eine Liste der verfügbaren Befehle.
3. Klicken Sie mit der rechten Maustaste auf den betreffenden Lenkungskalender und wählen Sie **Eigenschaften** aus.
   Dann wird die Eigenschaftsseite des Kalenders angezeigt.
4. Klicken Sie im Abschnitt **Lenkungsdaten** auf die Schaltfläche **Neu**.
   Das neue Lenkungsdatum wird in der Liste angezeigt.

Um die Merkmale des Lenkungsdatums zu definieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Eigenschaftsseite des Lenkungsdatums und wählen Sie die Registerkarte **Merkmale** aus.
2. Geben Sie den **Namen** des Datums an, um das Datum wieder eventuell in einem anderen Lenkungskalender zu verwenden.
3. Geben Sie den **Datumstyp** an.
   - "Anfang" - um den Beginn des Aktionsplans anzugeben
   - "Erinnerung" - um den Verantwortlichen an die Aktualisierung des Fortschritts zu erinnern
   - "Letzter" - um den Abschluss des Aktionsplans anzugeben
4. Geben Sie die Nachrichten an, die als Benachrichtigung und E-Mail gesendet werden sollen.
5. Wählen Sie die Registerkarte **Planung** aus.

6. Geben Sie das **Relative Referenzdatum** an, das im Vergleich zum **Effektiven Anfangsdatum** des Aktionsplans festgelegt wurde.
7. Geben Sie den **Intervalltyp** an, das angibt, in welchen Intervall die Erinnerungen gesendet werden: täglich, wöchentlich, monatlich, ein Mal.
8. Legen Sie das **Ende der Wiederholung** mit **kein Ende** fest.
9. Klicken Sie auf der Eigenschaftsseite des Lenkungsdatums auf **OK**.

Fortschrittsstatus eines Aktionsplans angeben

Um den Fortschrittsstatus eines Aktionsplans anzugeben, gehen Sie wie folgt vor:

1. Klicken Sie auf **Home > Mein Desktop > Meine Verantwortungsbereiche>Meine Aktionspläne**.
   Die Liste der Aktionspläne wird angezeigt.
2. Wählen Sie einen Aktionsplan aus und klicken Sie auf die Schaltfläche **Eigenschaften**.
3. Klappen Sie den Abschnitt **Fortschritt des Aktionsplans** auf.
4. Sie können die Prozente im Feld **Letzter Fortschritt (Prozent)** manuell aktualisieren.
5. Geben Sie den **Kommentar zum letzten Fortschritt** an.
6. Klicken Sie in der Tabelle **Fortschritt** auf **Neu**.
   Daraufhin wird die Seite zum Erstellen eines **Fortschritts** angezeigt.
7. Geben Sie den **Namen** des Fortschritts an.
8. Geben Sie den **Aktualisierten Fortschritt in Prozenten** an.
9. Überprüfen Sie das **Fortschrittsdatum**.
10. Geben Sie die **Bewertung des Fortschritts** an.
    - Verspätet
    - On Line
11. Klicken Sie auf der Eigenschaftsseite des Fortschrittsstatus auf **OK**.
    Der Status des Fortschritts wird in der Liste angezeigt.

Ablauf eines Aktionsplans in Schritten

☛ *Weitere Informationen zum Workflow finden Sie unter* *"Schritte im Workflow eines Aktionsplans", Seite 108**.*

Erstellung eines Aktionsplans

Sobald der Aktionsplan erstellt wird, hat er den Status "Zu senden".

Standardmäßig ist der Ersteller eines Aktionsplans auch der **Eigentümer** des Plans. Nachdem er die Merkmale des neuen Aktionsplans angegeben hat, kann der Ersteller:

- den Aktionsplan **senden**.
  In diesem Fall erhält der Benutzer, der als "Freigabeverantwortlicher" definiert wurde per E-Mail eine Benachrichtigung. Der neue Aktionsplan wird in der Aufgabenliste des Freigabeverantwortlichen mit dem Status "Zu starten" aufgeführt.

Vorbereitung eines Aktionsplans

Der Benutzer "Rechenschaftspflichtig" des Aktionsplans kann:

- den Aktionsplan **Starten**. Der Aktionsplan hat nun den Status "In Bearbeitung". Jetzt können Aktionen erstellt werden. Weitere Informationen finden Sie unter "Aktionen verwalten", Seite 79.

Ausführung des Aktionsplans

Nach Ausführung der Aktionen des Aktionsplans, kann der Benutzer "Verantwortlicher":

- den Aktionsplan **beenden**. Der Aktionsplan hat übernimmt den Status "Geschlossen", aber alle Aktionen des Aktionsplans müssen beendet sein. Weitere Informationen finden Sie unter "Aktionen verwalten", Seite 79.
  Der Benutzer "Freigabeverantwortlicher" wird über den Antrag, den Aktionsplan zu schließen, benachrichtigt.

Schließung des Aktionsplans

Nach Aufruf der Berichte über die Verfolgung des Aktionsplans, kann der Benutzer "Freigabeverantwortliche":

- den Aktionsplan **schließen**. Der Aktionsplan behält den Status "Geschlossen" bei und wird nicht mehr in der Aufgabenliste des Erstellers, des Freigabeverantwortlichen und des Eigentümers aufgeführt.
- **Wieder öffnen**, um weitere Aktionen durchzuführen. Der Aktionsplan hat nun den Status "In Bearbeitung".

AKTIONEN VERWALTEN

Der Eigentümer des Aktionsplans muss die Aktionen definieren, mit denen der Aktionsplan erfolgreich abgeschlossen werden kann. Er kann also Aktionen erstellen und zuweisen.

Eine Aktion ist in einem Aktionsplan enthalten und stellt eine Umwandlung oder eine Bearbeitung in einer Organisation oder einem System dar.

Aktionen erstellen

Um eine Aktion ab einem Aktionsplan zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Home > Mein Desktop > Meine Verantwortungsbereiche>Meine Aktionspläne**.
2. Wählen Sie auf der nun geöffneten Seite den betroffenen Aktionsplan aus und klicken Sie auf **Eigenschaften**.
3. Klicken Sie im Abschnitt **Aktionen** auf **Neu**.
   Die Aktion wird in der Liste der Aktionen des Aktionsplans aufgeführt.
4. Öffnen Sie das Eigenschaftsfenster der Aktionen und geben Sie den **Namen** der Aktion ein.
5. Geben Sie folgende Felder an:
   - **Priorität**: um eine Stufe anzugeben. Die Priorität kann verschiedene Stufen haben: "niedrig", "mittel", "hoch" oder "kritisch".
   - **Verantwortlicher einer Aktion**: für die Aktion verantwortlich, so wie er vom Ersteller der Aktion bestimmt wurde.
   - **Entitätseigentümer**: mit der Abteilung als Eigentümer kann die Liste der Eigentümer der Aktion eingegrenzt werden.
6. Geben Sie die Meilensteine an. Sie sind die wichtigen Daten der Aktion.
   - **Effektives Anfangsdatum** und **Geplantes Anfangsdatum**,
   - **Effektives Enddatum** und **Geplantes Enddatum**,
7. Klicken Sie auf **OK**.
   Die Aktion wird mit dem Status "Erstellt" erstellt.

Umfang der Aktion festlegen

Eine Aktion kann ein oder mehrere Objekte wie Kontrollen, Risiken oder Anwendungen betreffen.

Um zum Beispiel eine oder mehrere Kontrollen festzulegen, die im Rahmen der Aktion durchgeführt werden sollen, gehen Sie wie folgt vor:

1. Öffnen Sie die Eigenschaftsseite der Aktion.
2. Klappen Sie den Abschnitt **Umfang** auf.
3. Kontrollen verbinden, die eingerichtet werden sollen.

☛ *Auf diese Felder können Sie zugreifen, sobald die Aktion den Status "Geöffnet" hat.*

Schritte in der Verwaltung einer Aktion

☛ *Weitere Informationen zum Workflow finden Sie unter "Schritte im Workflow einer Aktion", Seite 111.*

Wenn eine Aktion erstellt wurde, muss sie vom Ersteller der Aktion als "Entwurf" angegeben werden.

Wenn alle Aktionen eines Aktionsplans veröffentlicht und akzeptiert wurden, kann der Aktionsplan umgesetzt werden.

Vorgeschlagener Befehl für den Ersteller

Wenn er die Merkmale einer neuen Aktion angegeben hat, kann "der Eigentümer oder Freigabeverantwortliche des Aktionsplans" folgenden Befehl verwenden:

- **Entwurf**.
  In diesem Fall erhält der Benutzer "Verantwortliche" eine Benachrichtigung. Die neue Aktion hat dann den Status "Entwurf".

Befehl, der für Entitäten vorgeschlagen wird, die von einer Aktion mit dem Status "Entwurf" betroffen sind

Wenn vom Benutzer eine Aktion vorgeschlagen wird, können "der Eigentümer und der Freigabeverantwortliche des Aktionsplans" und der Benutzer "Verantwortlicher":

- die Aktion **öffnen**. Die Aktion übernimmt den Status "Geöffnet".

Vorgeschlagene Befehle für den Verantwortlichen einer Aktion "Geöffnet"

Nach Überprüfung der Möglichkeiten, eine Aktion durchzuführen, kann der Benutzer "Verantwortliche":

- die Aktion **beenden**.
  Der Benutzer "Eigentümer und der Freigabeverantwortlicher des Aktionsplans" erhält eine Benachrichtigung.

Befehle, die dem "Eigentümer und Freigabeverantwortlichen des Aktionsplans" einer beendeteten Aktion vorgeschlagen werden

Nach Überprüfung der Merkmale der erstellten Aktion kann der "der Eigentümer und der Freigabeverantwortliche des Aktionsplans":

- **Schließen**.
  In diesem Fall erhält der Benutzer "Verantwortlicher" eine Benachrichtigung. Die Aktion hat dann den Status "Geschlossen".
- **An Verantwortlichen zurücksenden**, um zusätzliche Aktionen durchzuführen.

6

Die Berichte MEGA ERM

MEGA ERM bietet Funktionen für die Analyse und Verfolgung der Durchführung von Kontrollen und Risiken. Mit der **MEGA**-Suite können Objekt-Sets aus dem Repository in Berichten gruppiert werden und die Interaktion dieser Objekte geprüft werden.

☛ *Weitere Informationen zum Funktionsprinzip der Berichte finden Sie im Handbuch* ***MEGA Common Features*** *im Kapitel "Berichte generieren".*

Mit den standardmäßig von **MEGA ERM** angebotenen Berichtsvorlagen sollen die Kontrollen und Risiken analysiert werden. Mit den Berichtsvorlagen lassen sich die Analysen auf verschiedene Weisen darstellen.

In diesem Kapitel werden folgende Punkte behandelt:

Die Berichte über die Identifizierung

Kreuztabelle einer Aufteilung

In dieser Kreuztabelle werden die Verbindungen zwischen einer Liste von Risiken und Objekten eines bestimmten Typs angezeigt: Risikotyp, Entität, Prozess oder Ziel.

☛ *Weitere Informationen zur Kontextualisierung der Risiken finden Sie unter* *"Risiken organisieren", Seite 37.*

Berichtparameter

Hier werden die Eingabedaten des Berichts definiert.

Parameter	Parametertyp	Einschränkungen
Anfangsdatum	Datum	Auswahlkriterium der Risiken. Nicht obligatorisch
Enddatum	Datum	Auswahlkriterium der Risiken, auf das aktuelle Datum festgelegt.
Vererbter Kontext	Risikotyp, Entität, Prozess oder Ziel	Stamm der in Spalten aufgeführten Objekte. ***Obligatorisch***.
Zu verteilende Risiken	Liste der Risiken (ab einer Auswahl mit einem Risikotyp, einer Entität, einem Prozess oder einem Ziel).	Auswahlkriterium der Risiken. ***Obligatorisch***.

☛ *Die* ***zu verteilenden Risiken*** *können auch definiert werden, wenn Sie eine der folgenden Registerkarten auswählen:* ***Risiken verbinden***, ***Nach Entität verbinden***, ***Nach Prozess verbinden***, ***Nach Risikotyp verbinden*** *oder* ***Nach Ziel verbinden***.

Beispiel eines Berichts

Im folgenden Beispiel werden die Verbindungen zwischen einer Risikoliste und einer Liste der Unterentitäten der

Stammentität angezeigt, die im ***vererbten Kontext*** angegeben wurde.

	Logistics Department	Marketing Department	Regional Headquaters	Purchasing & Legal	Finance Department	Customer Satisfaction Department	Acc
Application Hack							
Change risks							
Contractual risks		✓					
Counterparty risks			✓		✓		
Cut-off				✓			
Default of payment					✓		✓
Lack of anticipation				✓			

Identifizierung der Risiken

Dieser Bericht führt die Aufteilung der Risiken auf mehrere Achsen auf: nach Prozess, nach Risikotyp, nach Entität und nach Ziel.

Berichtparameter

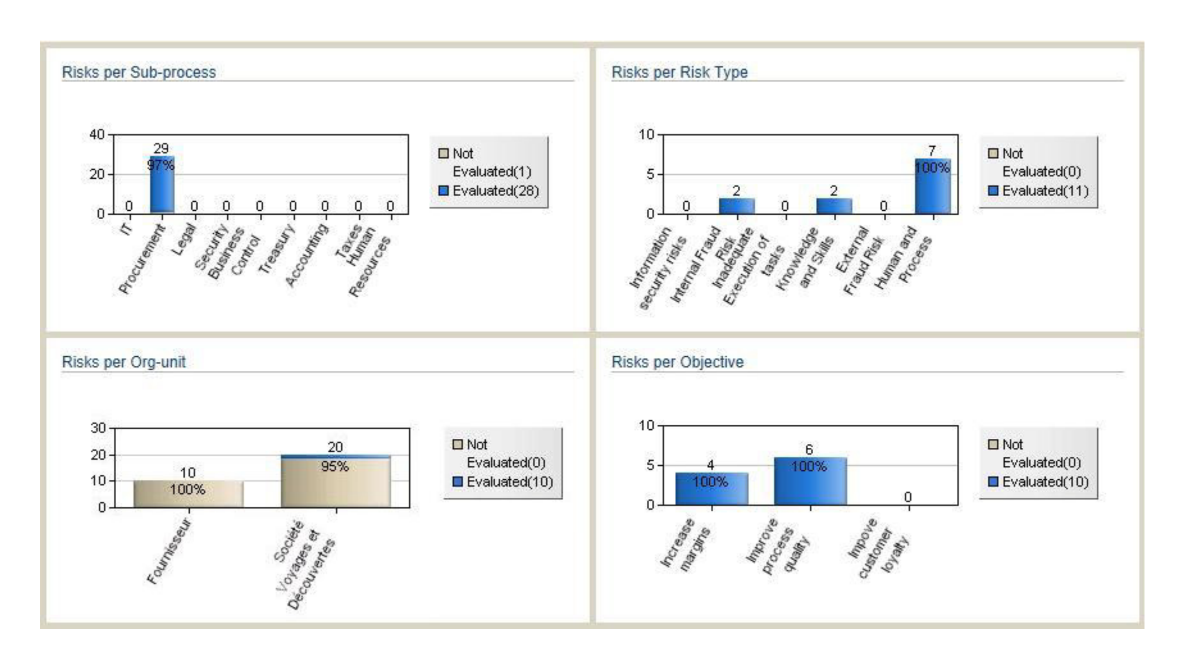
Hier werden die Risiken ausgewählt, die aufgeführt werden. Dabei werden die Elemente angegeben, die den Umfang der Risiken festlegen: Risikotypen, Entitäten, Prozesse oder Ziele.

Parameter	Parametertyp	Einschränkungen
Anfangsdatum	Datum	Auswahlkriterium der Risiken. Nicht obligatorisch
Enddatum	Datum	Auswahlkriterium der Risiken, auf das aktuelle Datum festgelegt.
Risikotypen des Umfangs	Risikotyp	Auswahlkriterium der Risiken. Nicht obligatorisch.
Entitäten des Umfangs	Entität	Auswahlkriterium der Risiken. Nicht obligatorisch.
Prozess des Umfangs	Prozesse	Auswahlkriterium der Risiken. Nicht obligatorisch.
Ziele des Umfangs	Ziele	Auswahlkriterium der Risiken. Nicht obligatorisch.

Beispiel eines Berichts

Im oberen Teil des Berichts wird die Aufteilung der Risiken nach folgenden Kriterien aufgeführt:

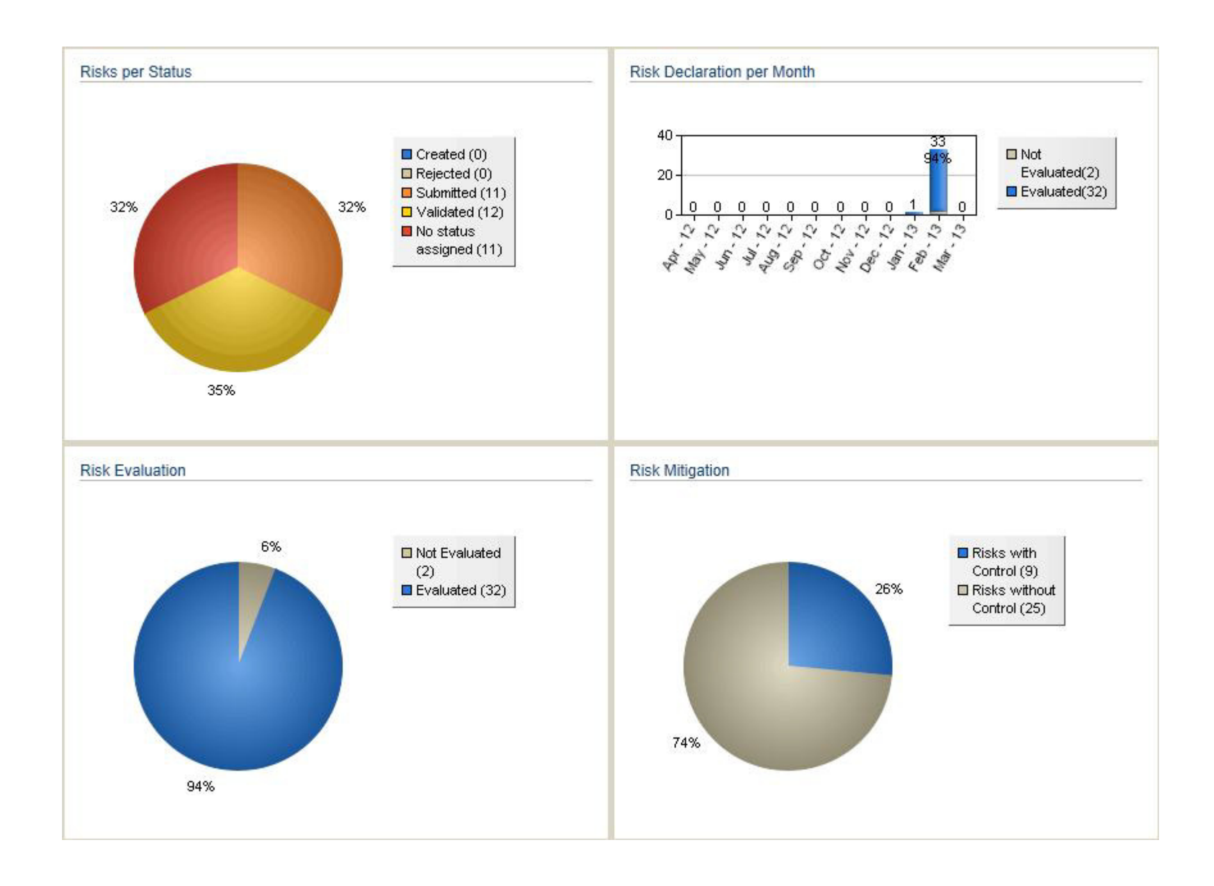
- Aufteilung der Risiken nach Prozessen
- Aufteilung der Risiken nach Risikotypen
- Aufteilung der Risiken nach Entitäten
- Aufteilung der Risiken nach Zielen



Im unteren Teil des Berichts wird die Aufteilung der Risiken nach folgenden Kriterien aufgeführt:

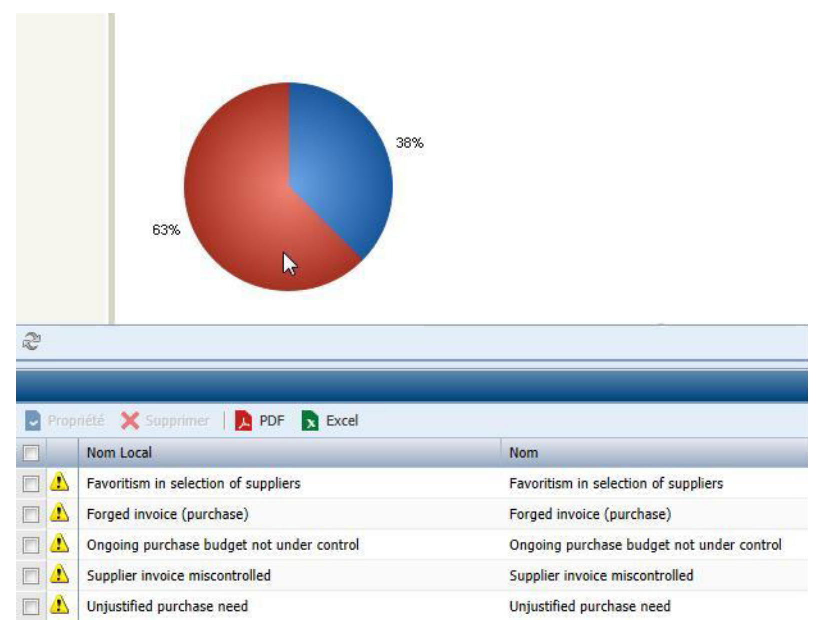
- Aufteilung der Risiken nach Status
- Aufteilung der Risiken, bei denen eine Bearbeitung definiert wurde
- Aufteilung der bewerteten und nicht bewerteten Risiken
- Anzahl der Risiken, die in den letzten zehn Jahren erstellt wurden.

☛ *Weitere Informationen zur Kontextualisierung der Risiken finden Sie unter "Risiken organisieren", Seite 37.*


Risks per Status
Created (0)
Rejected (0)
Submitted (11)
Validated (12)
No status assigned (11)
32%
32%
35%
Risk Declaration per Month
40
20
0
0 0 0 0 0 0 0 0 0 1 33 0
94%
Apr - 12
May - 12
Jun - 12
Jul - 12
Aug - 12
Sep - 12
Oct - 12
Nov - 12
Dec - 12
Jan - 13
Feb - 13
Mar - 13
Not Evaluated(2)
Evaluated(32)
Risk Evaluation
6%
94%
Not Evaluated (2)
Evaluated (32)
Risk Mitigation
26%
74%
Risks with Control (9)
Risks without Control (25)

Um eine Liste der Risiken zu erhalten, die einen Sektor oder einen Histogrammbalken bilden, gehen Sie wie folgt vor:

- Klicken Sie auf den betreffenden Sektor (bzw. Histogrammbalken).



Die Liste der Risiken wird unten in der Bearbeitungszone aufgeführt.

☛ *Weitere Informationen zur Funktionsweise der sofortigen Berichte finden Sie im Handbuch **MEGA Common Features**.*

Identifizierung der Kontrollen

Dieser Bericht führt die Aufteilung der Kontrollen auf mehrere Achsen auf: nach Prozess, nach Kontrolltyp, nach Entität und nach Ziel. Der Bericht funktioniert genauso wie der Bericht über die Identifizierung von Risiken.

☛ *Weitere Informationen zum Bericht über die Identifizierung von Risiken finden Sie unter "Identifizierung der Risiken", Seite 83.*

DIE AGGREGATIONEN

In Berichten über eine Aggregation wird eine Übersicht über die Bewertungsmessungen dargestellt, die bei den Risiken angegeben wurden.

Bei der Aggregation wird ein aggregierter Wert der Werte berechnet, die bei jedem Risiko an den Risikomessungen angegeben wurden.

Heatmap nach Entität / Risikotyp / Prozess

Mit diesem Bericht kann die Aufteilung der Risiken abhängig von folgenden Kriterien angezeigt werden:

- Auswirkung des Risikos im Vergleich zur Wahrscheinlichkeit, dass dieses Risiko eintritt
  - **Auswirkung**: bezeichnet die Auswirkung des Risikos, wenn es eintritt.
  - **Wahrscheinlichkeit**: bezeichnet die Wahrscheinlichkeit, dass das Risiko eintritt.
- Bruttorisiko im Vergleich zur Kontrollebene
  - **Bruttorisiko**: das Ergebnis des Auswirkunsgwerts multipliziert mit dem Wert der Wahrscheinlichkeit. Dieses Merkmal gibt Aufschluss über die Folgen des Risikos.
  - **Kontrollebene**: ist das Ergebnis des Werts des Designs der Kontrollen multipliziert mit dem Wert der Auswirkung der Kontrollen. Dieses Merkmal gibt einen globalen Aufschluss darüber, inwieweit das Risiko unter Kontrolle ist.

☛ *Weitere Informationen zur Bewertung von Risiken finden Sie unter "Bewertungen mit MEGA ERM", Seite 47.*

Berichtparameter

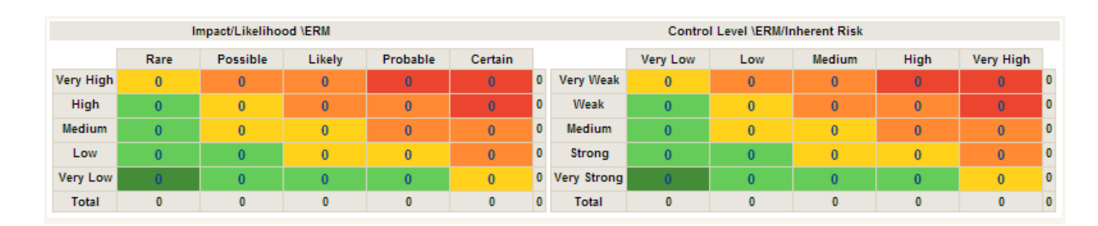
Hier werden die Eingabedaten des Berichts definiert.

Parameter	Parametertyp	Einschränkungen
Anfangsdatum	Datum	Auswahlkriterium der Risiken. Nicht obligatorisch
Enddatum	Datum	Auswahlkriterium der Risiken, auf das aktuelle Datum festgelegt.
Risikotyp des Kontextes	Risikotyp	Auswahlkriterium der Risiken. Nicht obligatorisch.

Parameter	Parametertyp	Einschränkungen
Entitäten des Kontextes	Entität	Auswahlkriterium der Risiken. Nicht obligatorisch.
Kontextprozess	Prozesse	Auswahlkriterium der Risiken. Nicht obligatorisch.
Kontextziele	Ziele	Auswahlkriterium der Risiken. Nicht obligatorisch.

Beispiel eines Berichts

Im folgenden Beispiel wurde kein Risiko bewertet.



Impact/Likelihood \ERM	Rare	Possible	Likely	Probable	Certain	
Very High	0	0	0	0	0	0
High	0	0	0	0	0	0
Medium	0	0	0	0	0	0
Low	0	0	0	0	0	0
Very Low	0	0	0	0	0	0
Total	0	0	0	0	0	0

Control Level \ERM/Inherent Risk	Very Low	Low	Medium	High	Very High	
Very Weak	0	0	0	0	0	0
Weak	0	0	0	0	0	0
Medium	0	0	0	0	0	0
Strong	0	0	0	0	0	0
Very Strong	0	0	0	0	0	0
Total	0	0	0	0	0	0

Die Berichte über eine Aggregation

Standardmäßig werden drei Typen von Aggregationsberichten angeboten:

- Aggregation der Risiken nach Entitäten
- Aggregation der Risiken nach Prozessen
- Aggregation der Risiken nach Risikotypen

☛ *Weitere Informationen zur Bewertung von Risiken finden Sie unter* *"Bewertungen mit MEGA ERM", Seite 47.*

Berichtparameter

Hier werden die Eingabedaten des Berichts definiert.

Parameter	Parametertyp	Einschränkungen
Anfangsdatum	Datum	Auswahlkriterium der Risiken. Nicht obligatorisch

Parameter	Parametertyp	Einschränkungen
Enddatum	Datum	Auswahlkriterium der Risiken, auf das aktuelle Datum festgelegt.
Stammobjekt	Je nach Berichttyp kann es sich beim Stammobjekt um eine Entität, einen Prozess oder einen Risikotyp handeln.	Im Bericht in Zeilen angezeigte Stammobjekte. ***Obligatorisch***.
Bewertete Merkmale	Bewertungsmerkmale.	Liste der Maße, die im Bericht in Spalten angezeigt werden. ***Obligatorisch***.

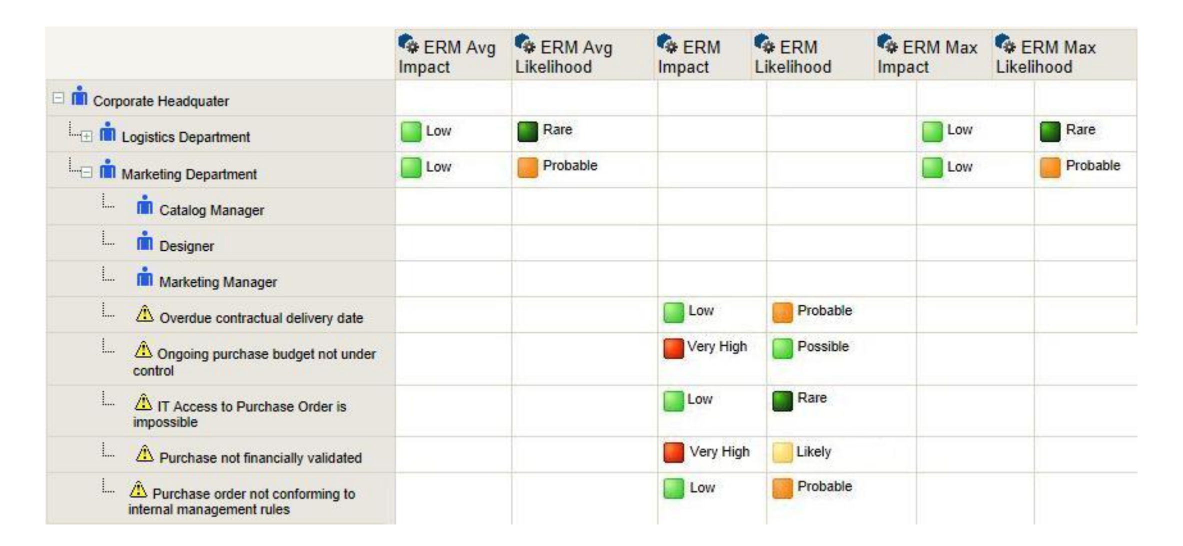
Beispiel eines Berichts

Im folgenden Beispiel werden die aggregierten Werte der Risiken bei Entitäten aufgeführt.



	ERM Avg Impact	ERM Avg Likelihood	ERM Impact	ERM Likelihood	ERM Max Impact	ERM Max Likelihood
Corporate Headquater						
Logistics Department	Low	Possible			Medium	Likely
Marketing Department	Very Low	Rare			Medium	Likely
Catalog Manager	Low	Possible			Medium	Likely
Designer	Very Low	Possible			Medium	Likely

Wenn eine Entität aufgeklappt wird, kann die Aggregation der Werte bei den einzelnen Risiken angezeigt werden, die mit der Entität verbunden sind.



	ERM Avg Impact	ERM Avg Likelihood	ERM Impact	ERM Likelihood	ERM Max Impact	ERM Max Likelihood
Corporate Headquater						
Logistics Department	Low	Rare			Low	Rare
Marketing Department	Low	Probable			Low	Probable
Catalog Manager						
Designer						
Marketing Manager						
Overdue contractual delivery date			Low	Probable		
Ongoing purchase budget not under control			Very High	Possible		
IT Access to Purchase Order is impossible			Low	Rare		
Purchase not financially validated			Very High	Likely		
Purchase order not conforming to internal management rules			Low	Probable		

DIE ÜBERWACHUNGSBERICHTE

Die Überwachungsberichte beziehen sich auf die Bewertungen und Aktionspläne.

Überwachung der Aktionspläne

In diesem Bericht wird die Aufteilung von Aktionsplänen nach Kriterien wie Prozessen und Entitäten sowie Art und Status der Prozesse aufgeführt.

☛ *Weitere Informationen zur Verwendung der Aktionspläne finden Sie unter "Aktionsplan beantragen", Seite 73.*

Berichtparameter

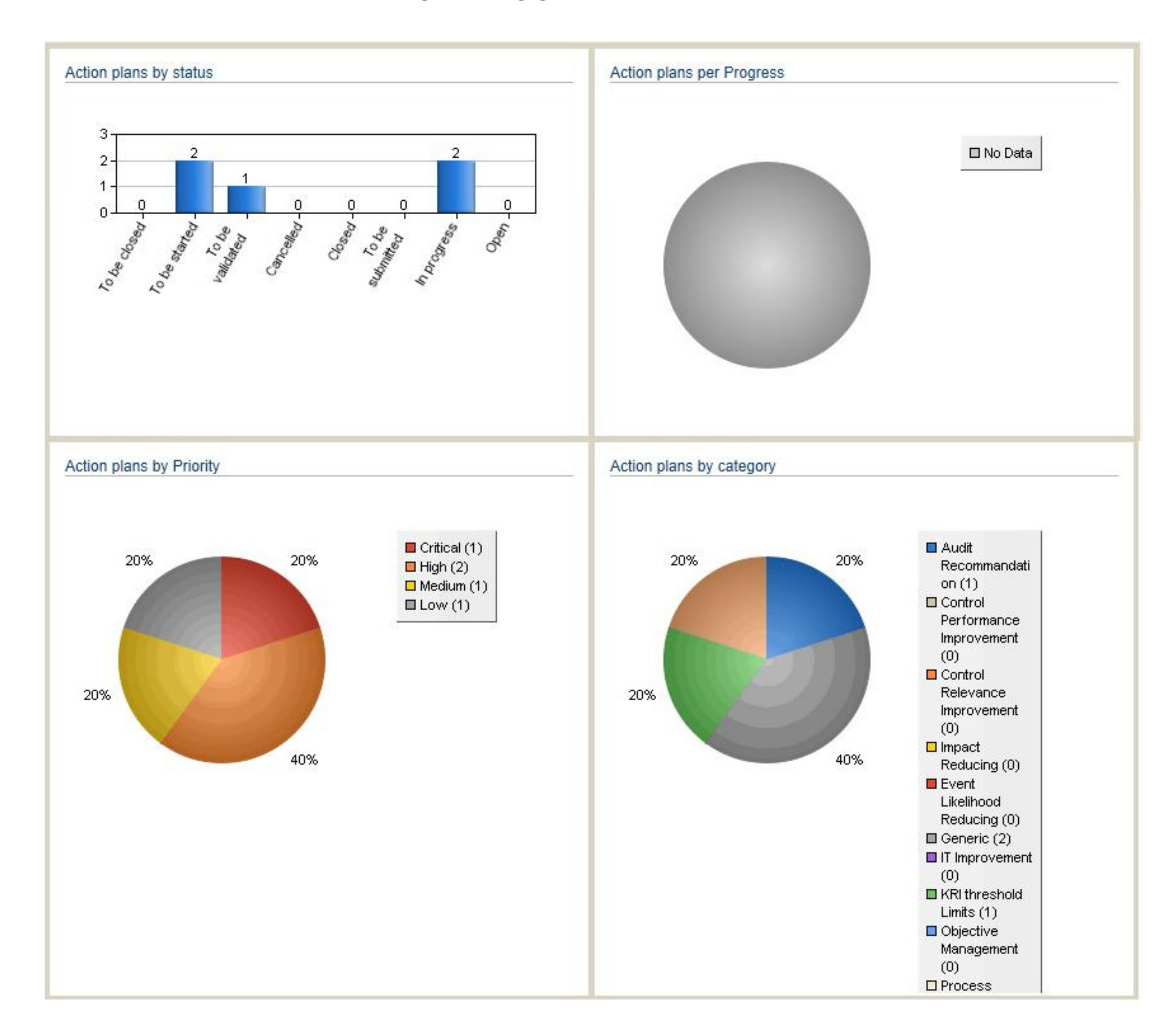
Hier werden Kontextelemente definiert, um die aufgeführten Aktionspläne auszuwählen. Die Aktionspläne beziehen sich nur auf die Entitäten und Prozesse, die in den Parametern angegeben wurden.

Parameter	Parametertyp	Einschränkungen
Anfangsdatum	Datum	Auswahlkriterium der Aktionspläne. Nicht obligatorisch
Enddatum	Datum	Auswahlkriterium der Aktionspläne, auf das aktuelle Datum festgelegt.
Entitäten	Entität	Auswahlkriterium der Aktionspläne. Nicht obligatorisch.
Prozess	Prozesse	Auswahlkriterium der Aktionspläne. Nicht obligatorisch.

Beispiel eines Berichts

Im oberen Teil des Berichts wird die Aufteilung der Aktionspläne nach folgenden Kriterien aufgeführt:

- Aufteilung abhängig von der Art
- Aufteilung abhängig vom Fortschritt
- Aufteilung abhängig von den Kategorien
- Aufteilung abhängig von den Prioritäten



Im unteren Teil des Berichts wird die Aufteilung der Aktionspläne nach folgenden Kriterien aufgeführt:

- Aufteilung nach Art
- Aufteilung nach Prozessen
- Aufteilung nach Entitäten

☛ *Um die Liste der Risiken zu erhalten, die einen Sektor oder einen Histogrammbalken bilden, klicken Sie auf den betreffenden Sektor (bzw. Histogrammbalken).*

Statistiken einer Sitzung

In diesem Bericht wird die Aufteilung der Antworten einer Bewertungssitzung analysiert.

☛ *Weitere Informationen zur Verwendung der Aktionspläne finden Sie unter "Bewertungssitzung verwalten", Seite 62.*

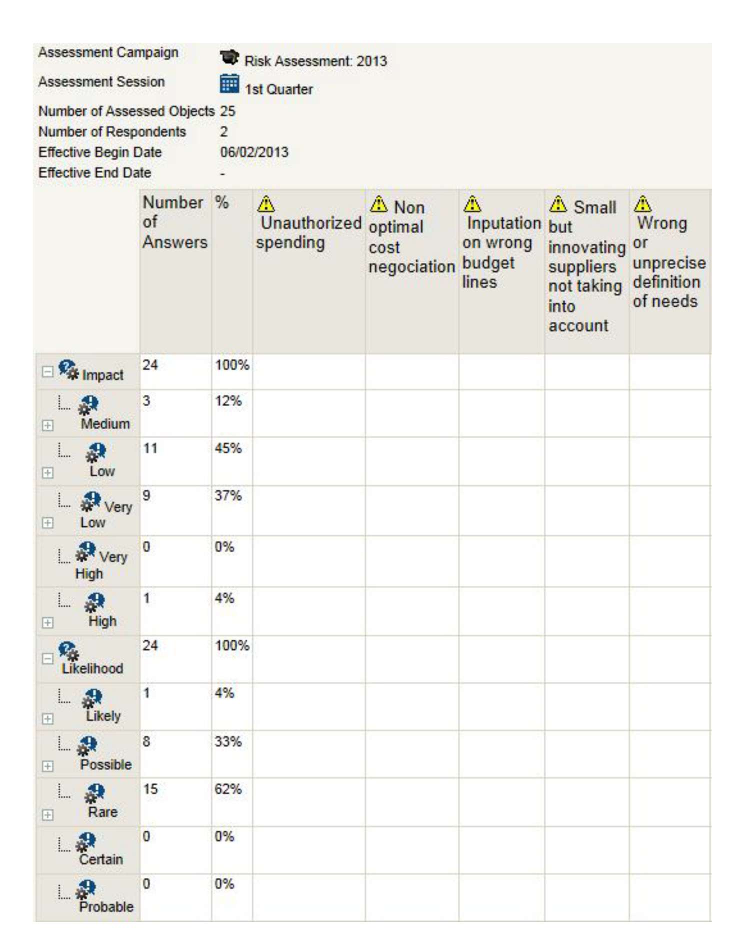
Berichtparameter

Hier wird die Sitzung ausgewählt, auf die sich die Analyse bezieht.

Parameter	Parametertyp	Einschränkungen
Kampagne	Kampagne	***Obligatorisch***.
Sitzung	Sitzung	***Obligatorisch***.

Beispiel eines Berichts

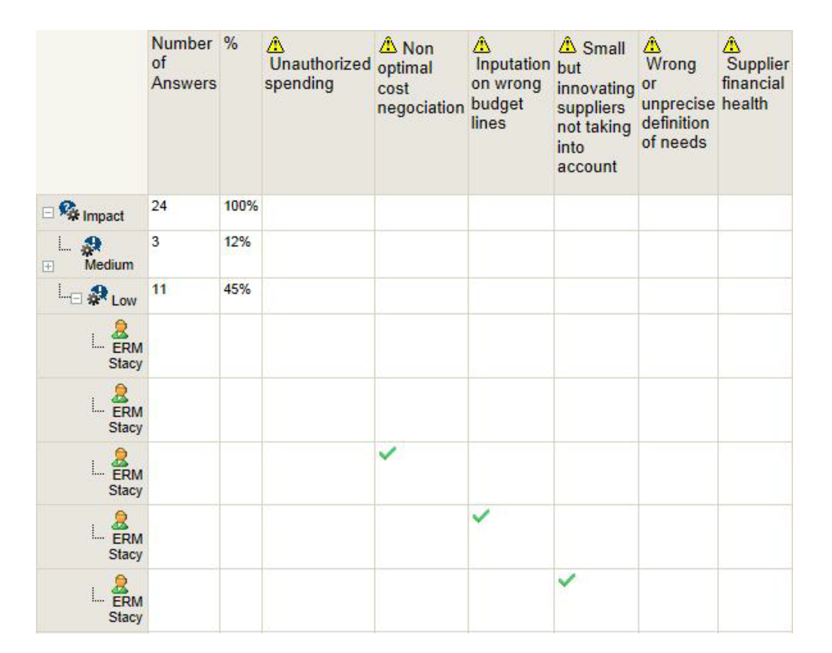
Im folgenden Beispiel wird die Aufteilung der Antworten bei zwei Merkmalen einer Risikobewertung aufgeführt (Auswirkung und Periodizität).



Assessment Campaign	Risk Assessment: 2013
Assessment Session	1st Quarter
Number of Assessed Objects	25
Number of Respondents	2
Effective Begin Date	06/02/2013
Effective End Date	-

	Number of Answers	%	Unauthorized spending	Non optimal cost negociation	Inputation on wrong budget lines	Small but innovating suppliers not taking into account	Wrong or unprecise definition of needs
Impact	24	100%					
Medium	3	12%					
Low	11	45%					
Very Low	9	37%					
Very High	0	0%					
High	1	4%					
Likelihood	24	100%					
Likely	1	4%					
Possible	8	33%					
Rare	15	62%					
Certain	0	0%					
Probable	0	0%					

Wenn eine Antwort aufgeklappt wird, werden der Name des Bewerters sowie die Risiken aufgeführt, auf die sich die Antwort bezieht.



	Number of Answers	%	Unauthorized spending	Non optimal cost negociation	Inputation on wrong budget lines	Small but innovating suppliers not taking into account	Wrong or unprecise definition of needs	Supplier financial health
Impact	24	100%						
Medium	3	12%						
Low	11	45%						
ERM Stacy								
ERM Stacy								
ERM Stacy				✓				
ERM Stacy					✓			
ERM Stacy						✓		

Effizienz des Risikomanagements

Risikominderung

In diesem Bericht wird die Entwicklung des Nettorisikos zwischen zwei Daten aufgeführt, um die Vorteile der durchgeführten Aktionspläne zu analysieren.

☛ *Weitere Informationen zur Verwendung der Risikobewertung finden Sie unter* *"Bewertungen mit MEGA ERM", Seite 47**.*

Berichtparameter

Hier werden Kontextelemente definiert, um die im Bericht aufgeführten Risiken auszuwählen. Die Risiken beziehen sich nur auf die Entitäten und Prozesse, die in den Parametern angegeben wurden.

Parameter	Parametertyp	Einschränkungen
Anfangsdatum	Datum	Anfangsdatum. ***Obligatorisch***.
Enddatum	Datum	Enddatum. ***Obligatorisch***.
Entitäten	Entität	Auswahlkriterium der überprüften Risiken. Nicht obligatorisch.
Prozess	Prozesse	Auswahlkriterium der überprüften Risiken. Nicht obligatorisch.

Beispiel eines Berichts

Context	Risk	ERM Avg Net Risk 2012	Action plans	ERM Avg Net Risk 2013
	Application Hack			Low
	Risk of dependency	Very High		
	Unprecise measurement of the procurement department			Medium
	Insufficient market analysis	High		
	Purchase from unathorized providers	Medium		Medium
	Supplier financial health	Medium		Medium
	Risk of non payment	Low		Medium
	Small but innovating suppliers not taking into account	Medium		Low
	Fraud: unregistered call for tender	High		
	Lack of anticipation	Low		
	Wrong or unprecise definition of needs			Medium
	Insufficient budget	High		
	Inputation on wrong budget lines	High		
	Purchase of unauthorized material	High		Low
	Non optimal cost negociation	Medium		Low
	Non compliance with legal context	High		Low

TRENDANALYSE

Trendanalyse

In diesem Bericht wird die Entwicklung des Nettorisikos der letzten drei Jahre sowie des kommenden Jahrs aufgeführt. Dazu werden der Durchschnittswert und der maximale Wert des Nettorisikos verwendet.

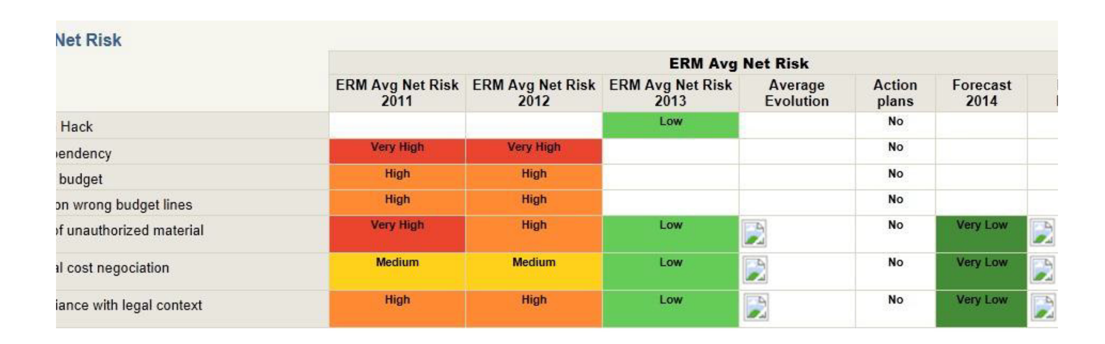
☛ *Weitere Informationen zur Verwendung der Risikobewertung finden Sie unter "Bewertungen mit MEGA ERM", Seite 47.*

Berichtparameter

Hier wird der Kontext der aufgeführten Risiken definiert.

Parameter	Parametertyp	Einschränkungen
Kontext des Berichts	Risikotyp, Entität, Prozess oder Ziele	Auswahlkriterium der in Zeilen angezeigten Risiken. Nicht obligatorisch.

Beispiel eines Berichts



Net Risk

	ERM Avg Net Risk						
	ERM Avg Net Risk 2011	ERM Avg Net Risk 2012	ERM Avg Net Risk 2013	Average Evolution	Action plans	Forecast 2014	
Hack			Low		No		
endency	Very High	Very High			No		
budget	High	High			No		
on wrong budget lines	High	High			No		
f unauthorized material	Very High	High	Low		No	Very Low	
l cost negociation	Medium	Medium	Low		No	Very Low	
iance with legal context	High	High	Low		No	Very Low	

GLOSSAR

Aggregationsschema Ein Aggregationsschema ist eine Reihe von Schritten, mit denen die Ergebnisse einer Bewertung nach festgelegten Bewertungsregeln konsolidiert werden.

Aktion Eine Aktion ist in einem Aktionsplan enthalten und stellt eine Umwandlung oder eine Bearbeitung in einer Organisation oder einem System dar.

Aktionsplan Ein Aktionsplan besteht aus einer Reihe von Aktionen. Der Aktionsplan soll die Risiken oder Ereignisse reduzieren, die sich auf die Aktivitäten des Unternehmens negativ auswirken bzw. die Effizienz eines Prozesses oder einer Organisation verbessern können.

Anforderung Eine Anforderung ist ein explizit ausgedrückter Bedarf oder eine Erwartung, die wie eine Einschränkung vorgeschrieben und im Rahmen eines Zertifikations-, Organisations- oder Modifikationsprojekts für das Informationssystem des Unternehmens erfüllt werden muss.

Anwendung Eine Anwendung besteht aus Software-Komponenten, die im Rahmen der IT-Entwicklungen eine konsistente Einheit bilden.

Arbeitsschritt Ein Arbeitsschritt ist eine Etappe eines Ablaufs, bei der eine Organisationseinheit der Organisation im Rahmen einer der Aktivitäten des Unternehmens handelt. Es kann sich hier um einen industriellen Arbeitsschritt handeln, wie „ein Teil fertigen", um einen logistischen Arbeitsschritt, wie „eine Lieferung annehmen", oder auch um eine Informationsverarbeitung, wie „eine Bestellung speichern". Ein Arbeitsschritt kann in elementare Aufgaben aufgeteilt werden.

Benutzer Ein Benutzer ist eine Person (oder eine Personengruppe) mit einem Login. Ein Benutzer verfügt über eine gewisse Anzahl von Zugriffsrechten für die Produktfunktionalitäten und Repositorys. Der Benutzer verfügt insbesondere in jedem Repository über einen eigenen Arbeitsbereich, mit dem er sich ab jedem beliebigen Arbeitsplatz einer gegebenen Umgebung verbinden kann. Der mit dem Benutzer während seiner Erstellung verknüpfte Code wird zum Erstellen verschiedener Dateinamen und insbesondere für sein Arbeitsverzeichnis verwendet. Standardmäßig können bei der Installation mit den Personen Administrator (Login: System) und Mega (Login: Mega) die Repositorys so administriert werden, dass neue Benutzer erstellt werden.

Bewertetes Merkmal Ein bewertetes Merkmal legt fest, was bei einer Bewertung bewertet werden soll. Das Merkmal kann mit einer MetaClass verbunden werden, vor allem mit einem der MetaAttributs, zum Beispiel. Metaclasse Risiko, MetaAttribut: Wahrscheinlichkeit.

Bewertung Die Bewertung ist ein Mechanismus, mit dem einer identifizierten Population Fragebögen zugesendet werden, um (qualitative oder quantitative) Einschätzungen von identifizierten Objekten zu erhalten. Die Bewertung wird durch Werkzeuge für die Ergebnisanalyse ergänzt.

Bewertungssitzung Eine Bewertungssitzung ist eine Bewertung, die zu einem bestimmten Zeitpunkt gestartet wird. Mit der Veröffentlichung der Bewertungssitzung soll ein Bewertungsfragebogen gesendet werden, in dem die Fragen gezielt an die Bewerter gerichtet werden.

Bewertungsvorlage Eine Bewertungsvorlage dient als Vorlage zur Erstellung von Bewertungskampagnen und -sitzungen. Die Bewertungsvorlage legt den Umfang der Bewertung fest, sowie die zu verwendende Fragebogenvorlage und eventuell die Aggregationsschemen, die für die Auslegung der globalen Ergebnisse verwendet werden.

Bruttorisiko Ein Bruttorisiko bezeichnet ein Risiko für ein Unternehmen, wenn keine Maßnahmen getroffen werden, die Wahrscheinlichkeit oder Auswirkung dieses Risikos zu ändern.

Datenbank Eine Datenbank ermöglicht, die logische oder physische Speicherungsstruktur der Daten anzugeben.

Empfehlung Eine Empfehlung beschreibt, was zur Behebung von nicht-konformen Fakten durchgeführt werden muss, die während eines Audits festgestellt wurden.

Entität

Eine Entität kann unternehmensintern oder -extern sein: Eine Entität stellt ein Element der Struktur eines Unternehmens dar, wie beispielsweise eine Direktion, eine Abteilung oder einen Arbeitsplatz. Sie wird auf einer mehr oder weniger genauen Ebene definiert, je nachdem, wie präzise die Angaben über die Organisation sein müssen (siehe Organisationseinheitstyp). Beispiel: Finanzdirektion, Vertrieb, Marketingabteilung, Vertriebsmitarbeiter. Eine externe Entität stellt eine Einrichtung dar, die Flüsse mit dem Unternehmen austauscht. Beispiel: Kunde, Lieferant, Administration.

Ereignis

Ein Ereignis ist ein Fakt einer internen oder externen Quelle, der sich auf die Organisation auswirkt. Er bildet das Grundelement für die Sammlung von Daten über ein Betriebsrisiko.

Fragebogen

In einem Fragebogen wird eine Liste von vordefinierten Fragen aufgeführt, die für einen Ereignistyp, eine Kontrolle, ein Dokument usw. gelten können.

Fragebogenvorlage

Eine Fragebogenvorlage entspricht der Definition des Inhaltes eines Fragebogens: Fragegruppe, Fragen, einmalige oder mehrere Antworten und mögliche Antworten. Die Fragebogenvorlage kann mit der Präsentation eines Fragebogens verbunden werden, die die Anzeigeoptionen angibt. Die an die Bewerter gesendeten Fragebögen werden ab der Definition generiert, die in der Fragebogenvorlage geliefert wird.

Geschäftsprozess

Ein Geschäftsprozess stellt ein System dar, das Produkte oder Dienstleistungen an einen internen oder externen Kunden des Unternehmens oder Organisation liefert. Auf höherer Ebene definiert ein Geschäftsprozess eine Strukturierung und Kategorisierung des Geschäftsbereichs eines Unternehmens. Der Geschäftsprozess kann in weitere Prozesse unterteilt werden. Mit der Verbindung zu den organisatorischen Prozessen kann die reelle Implementierung des Geschäftsprozesses in der Organisation beschrieben werden. Ein Geschäftsprozess kann auch mit einer funktionalen Sicht detailliert werden.

Geschäftsrollen

Eine Geschäftsrolle definiert die Funktion einer Person im geschäftlichen Bereich. Eine Person kann mehrere Geschäftsrollen übernehmen. Geschäftsrollen werden nur verwendet, wenn die Option "Verwaltung der Zuweisung von Geschäftsrollen an Personen" aktiviert wurde. Ein Profil kann mit einer Geschäftsrolle verbunden sein. Wenn eine Person einer Geschäftsrolle zugewiesen wird, die mit einem Profil verknüpft ist, wird dieser Person indirekt ein Profil zugewiesen.

Geschäftssparte Eine Geschäftssparte ist eine hohe Klassierungsebene der wichtigsten Geschäftstätigkeiten eines Unternehmens. Sie entspricht zum Beispiel großen Produktsegmenten oder Distributionskanälen. Sie ermöglicht, Prozesse eines Unternehmens, organisatorische Einheiten oder Anwendungen für ein bestimmtes Produkt und/oder einen bestimmten Markt zu klassieren. Regelwerke bestimmter Industrien schreiben ihre eigene Liste von Geschäftssparten vor.

Gesellschaft Eine Gesellschaft ist eine juristische Person.

Indikator Ein Indikator ist eine messbare Größe, die Angaben über das erreichte oder nicht erreichte Ziel, die Auswirkung eines Risikofaktors, die Häufigkeit oder die Auswirkung eines Risikos, die Wirksamkeit einer Kontrolle usw. liefert.

Kampagne In einer Kampagne können mehrere Bewertungssitzungen gruppiert werden.

Kontrolle Eine Kontrolle ist ein Mittel, ein oder mehrere Risiken unter Kontrolle zu haben, und sicherzustellen, dass eine gesetzliche, vorschriftsmäßige oder interne Anforderung des Unternehmens erfüllt wird.

Kontrolltyp Mit einem Kontrolltyp lassen sich die Kontrollen klassieren, die im Unternehmen entsprechend des Standards bzw. Normen der betreffenden Sektoren oder Vorschriften/Reglementierungen (Cobit usw.) implementiert sind.

Lenkungsdatum Ein Lenkungsdatum ist ein Datum, das in einem Lenkungskalender festgelegt wird und an dem der verantwortlichen Person eines Elements eine Erinnerung gesendet wird. Ein Anfangsdatum, ein Erinnerungsdatum oder ein Termin (Enddatum).

Lenkungskalender Mit dem Lenkungskalender können wiederholte Aktionen zu vordefinierten Terminen durchgeführt werden. Man kann den Kalender zum Beispiel verwenden, um Erinnerungen an die Person zu senden, die für einen Aktionsplan verantwortlich ist, damit sie den Fortschritt angibt, der bei diesem Aktionsplan erzielt wurde. Man kann einen Lenkungskalender auch verwenden, um den Start von Bewertungssitzungen zu regelmäßigen Terminen auszulösen ...

Maß Ein Maß liefert mengenbezogene Angaben über den Wert einer Größe (zum Beispiel die Höhe einer Risikoprävention).

Organisatorische r Prozess Ein organisatorischer Prozess beschreibt die Schritte, die durchgeführt werden müssen, um den Prozess zur Herstellung eines Produkts oder Flusses insgesamt oder teilweise umzusetzen.

Person Eine Person wird mit ihrem Namen und ihrer E-Mail-Adresse definiert. Um auf **MEGA** zuzugreifen, kann eine Person auf das Produkt zugreifen, sobald sie eine ID (Login) zur Verbindung erhalten hat. Auch eine oder mehrere Geschäftsrollen können der Person zugewiesen werden. Diese Personenliste kann zum Beispiel von einem LDAP-Server stammen.

Produkt Ein Produkt stellt einen oder mehrere Artikel, Objekte, Produkte oder Dienstleistungen als Ergebnis einer Aktivität in der Landwirtschaft, der Industrie oder des Dienstleistungsbereichs dar, die von einem Unternehmen angeboten werden.

Profil Ein Profil definiert, was eine Person sehen bzw. in den Tools machen darf oder nicht und wie er es sieht und machen darf. In einem Profil werden die Optionen, die Zugriffsrechte für Repositorys und Produkte und die Rechte für den Schreibschutz bzw. zum Einlesen der Objekte definiert. Alle Benutzer mit demselben Profil haben dieselben Optionen und Rechte.

Prozesse Ein Prozess ist eine Wertekette, die einem internen oder externen Kunden Güter oder Services bereitstellt. Diese Wertekette wird durch eine Folge von Aktivitätsumwandlungen beschrieben. Sie wird von den Abläufen implementiert.

Redundanz der Kontrollen Eine Redundanz der Kontrollen formalisiert die Tatsache, dass sich mehrere Kontrollen wiederholen. Zum Beispiel weil sie nacheinander eingerichtet wurden, um ein Risiko im Rahmen unterschiedlicher Vorschriften zu decken.

Restrisiko Ein Restrisiko ist ein Risiko, das für ein Unternehmen besteht, wenn das Management auf das Risiko reagiert, d.h. bearbeitet.

Risiko Ein Risiko ist eine mehr oder weniger wahrscheinliche Gefahr, der einer Organisation ausgesetzt ist.

Risiko- und Kontrollsystem Ein Kontrollsystem besteht aus mehreren Kontrollen, mit denen Risiken für ein Unternehmen verhütet und Risiken unter Kontrolle gehalten werden können, sowie interne Betriebsregeln angewendet, Gesetze oder Vorschriften eingehalten oder strategische Ziele des Unternehmens erreicht werden können.

Risikofaktor	Ein Risikofaktor ist ein Element, das zum Auftreten eines Risikos beiträgt oder ein Risiko auslöst. Für verschiedene Risiken kann ein und derselbe Risikofaktor verantwortlich sein. Beispiele: Die Verwendung eines gefährlichen chemischen Produkts, eine komplexe Anwendung, die Größe eines Projekts, die Anzahl der Mitwirkenden, eine neue Technik, mangelnde Qualitätssicherung, mangelnde Sorgfalt bei der Festlegung der Anforderungen usw.
Risikofolge	Die Folge eines Risikos kann positiv oder negativ sein. Sie wird mit einem Typ verbunden, mit dem sich die Folge charakterisieren lässt. Beispiel: Bild, Umgebung, Angestellte.
Risikotyp	Ein Risikotyp definiert die Typologie eines normalisierten Risikos im Rahmen einer Organisation.
Server	Ein Server ist eine Hardware-Ressource, die über eine Datenbank verfügen kann, auf der eine Anwendung ausgeführt werden kann.
Vorschriften oder interne Regelung	Eine Vorschrift oder eine interne Regelung stellt mehrere Richtlinien mit oder ohne Bedingungen auf, die von der Regierung im Rahmen eines Gesetzes, von einem Berufsverband in Form von Best Practices oder intern von einer Organisation festgelegt werden.
Ziel	Ein Ziel ist ein Ergebnis, das erreicht werden soll, oder das angestrebte Resultat eines Prozesses oder eines Arbeitsschritts. Mit einem Ziel können die Punkte hervorgehoben werden, die für diesen Prozess oder diesen Arbeitsschritt verbessert werden sollen.

8

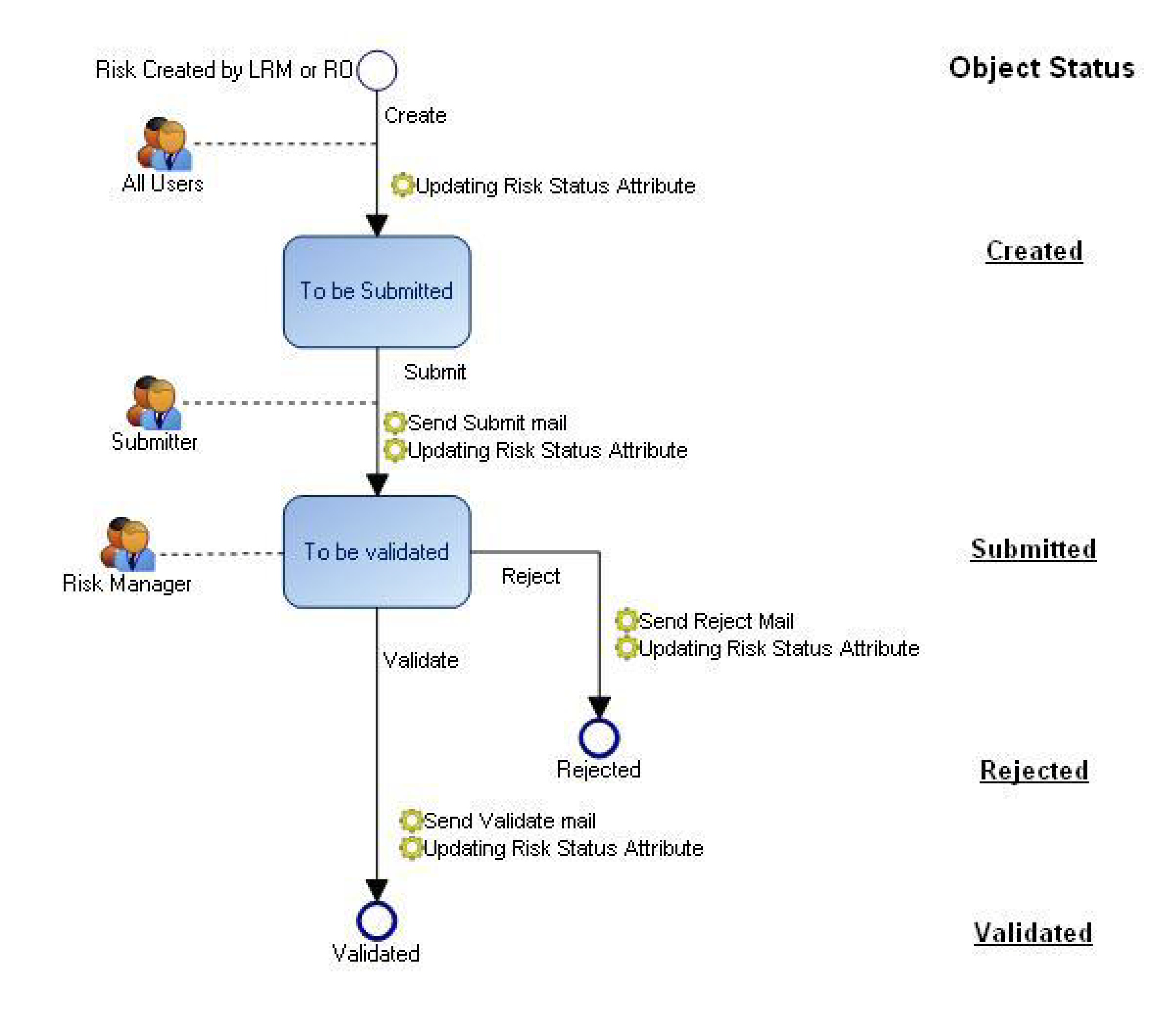
ANHANG - WORKFLOW VON MEGA ERM

In diesem Kapitel werden die Workflow-Diagramme von **MEGA ERM** aufgeführt.

WORKFLOW EINES RISIKOS

Schritte im Workflow bei der Erstellung einer Kontrolle

Die Schritte des Freigabeprozesses einer neuen Kontrolle werden im Absatz "Prozess der Erstellung eines Risikos", Seite 35 beschrieben.



E-Mails im Workflow bei der Erstellung eines Risikos

Anforderung der Freigabe eines Risikos

Von	Eigentümer des Risikos
An	Risikomanager
Gegenstand	Risk to be validated - [Current risk Name]
Inhalt	Please validate the risk: [Current risk Name]. To enter the application and perform your task, [Click here]. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.

Risiko freigeben

Von	Risikomanager
An	Eigentümer des Risikos
Gegenstand	Your risk has been approved - [Current risk Name]
Inhalt	The risk [Current risk Name] has been approved by The Risk Management Department. Thank you for your collaboration. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.

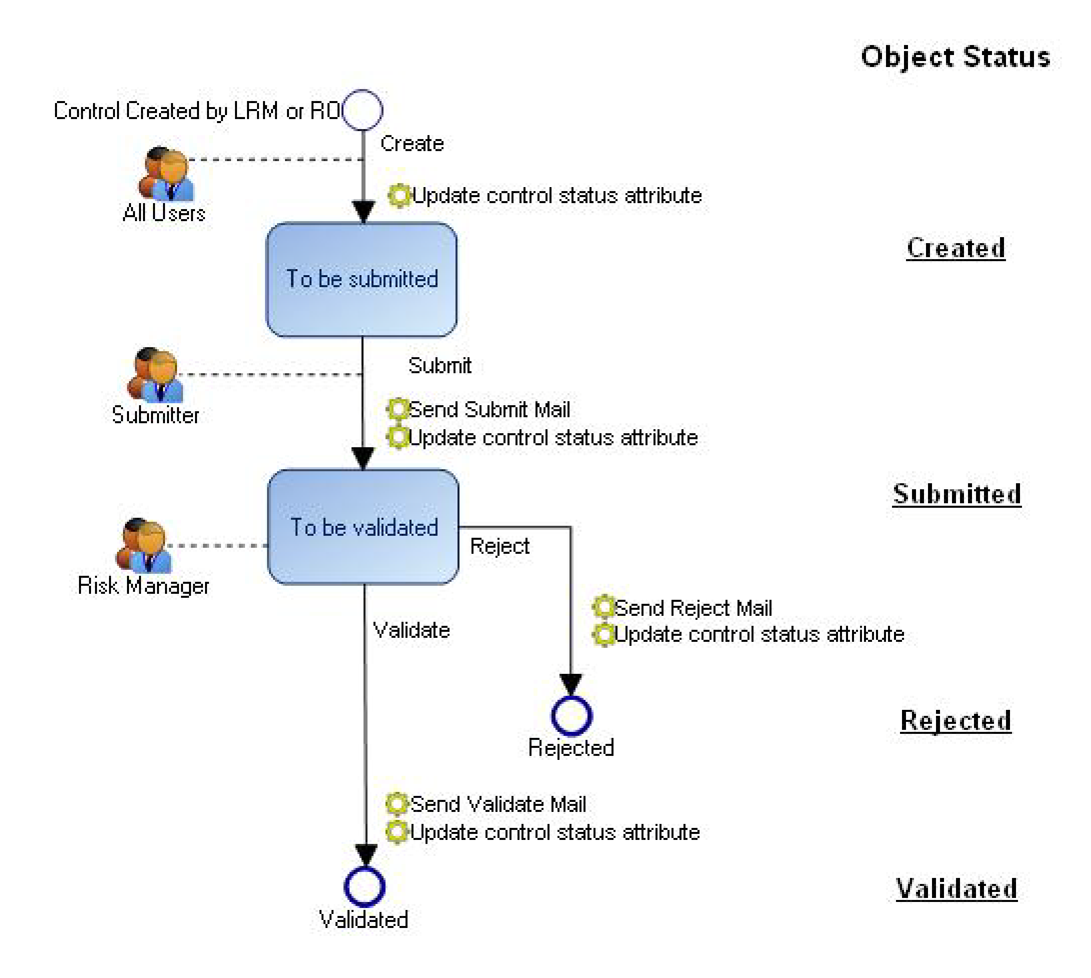
Risiko zurückweisen

Von	Risikomanager
An	Eigentümer des Risikos
Gegenstand	Your risk has been rejected - [Current risk Name]
Inhalt	The risk [Current risk Name] has been rejected by The Risk Management Department. Thank you for your collaboration. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.

WORKFLOW EINER KONTROLLE

Schritte im Workflow bei der Erstellung einer Kontrolle

Die Schritte des Freigabeprozesses einer neuen Kontrolle werden im Absatz "Kontrolle erstellen", Seite 45 beschrieben.



E-Mails im Workflow bei der Erstellung einer Kontrolle

Anforderung der Freigabe einer Kontrolle

Von	Eigentümer der Kontrolle
An	Risikomanager
Gegenstand	Control to be validated - [Current control Name]
Inhalt	Please validate the control: [Current control Name]. To enter the application and perform your task, [Click here]. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.

Kontrolle freigeben

Von	Risikomanager
An	Eigentümer der Kontrolle
Gegenstand	Your control has been approved - [Current control Name]
Inhalt	The control [Current control Name] has been approved by The control Management Department. Thank you for your collaboration. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.

Kontrolle zurückweisen

Von	Risikomanager
An	Eigentümer der Kontrolle
Gegenstand	Your control has been rejected - [Current control Name]
Inhalt	The control [Current control Name] has been rejected by The Risk Management Department. Thank you for your collaboration. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.

Workflow eines Aktionsplans

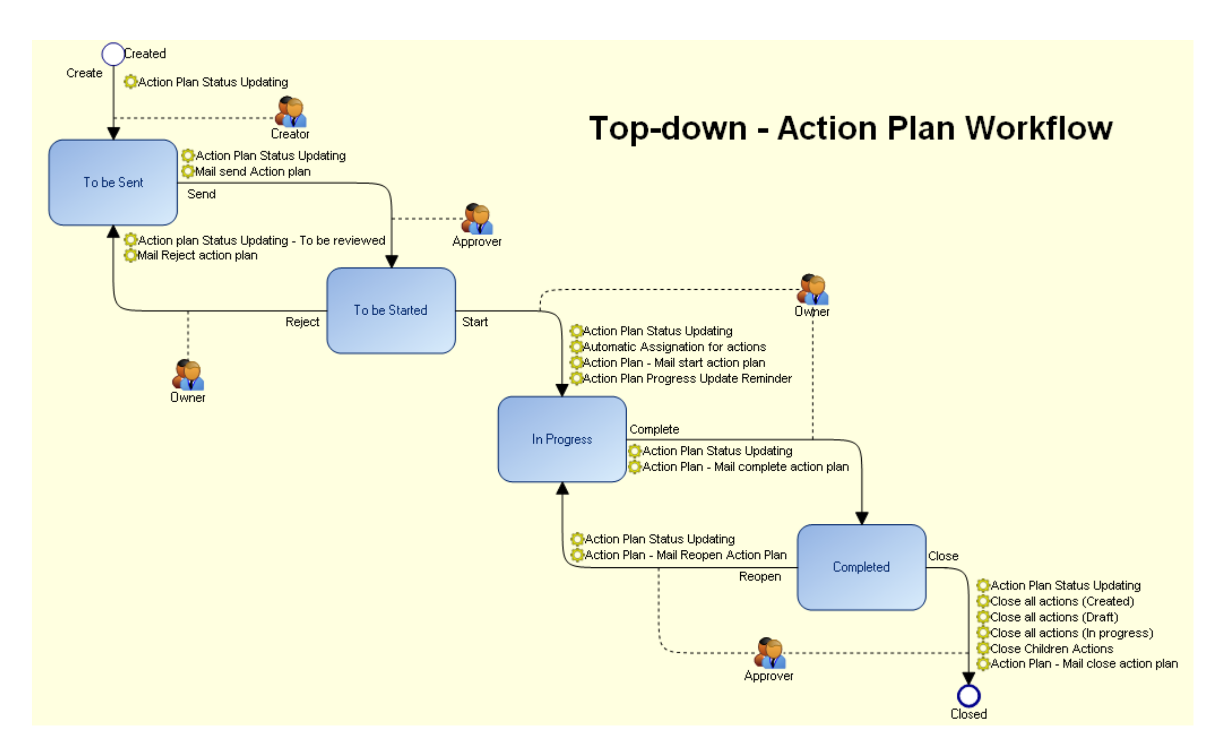
Schritte im Workflow eines Aktionsplans

Die Schritte des Verwaltungsprozesses eines Aktionsplans werden im Absatz "Ablauf eines Aktionsplans in Schritten", Seite 77 beschrieben.

Das Workflow-Diagramm führt auf:

- die mitwirkenden Personen
  - der "Ersteller", der auch die Schließung des Aktionsplans freigibt
  - der "Rechenschaftspflichtige", der für die Durchführung der Aktionen des Aktionsplans ist
  - der '"Freigabeverantwortliche", der für den Umfang verantwortlich, der vom Aktionsplan abgedeckt wird.
- die Statusangaben des Workflows des Aktionsplans sowie die geplanten Transitionen von einem Status zum anderen
- die geplanten Benachrichtigungen bei bestimmten Transitionen.

Workflow des Aktionsplans



E-Mails im Workflow eines Aktionsplans

Freizugebender Aktionsplan

Von	Ersteller
An	Freigabeverantwortlicher
Gegenstand	Action plan to be validated - [Current Action plan Name]
Inhalt	Please validate the action plan submitted by [Action Plan Creator Name] . To enter the application and perform your task, [Click here]. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.

Freigegebener Aktionsplan

Von	Freigabeverantwortlicher
An	Ersteller
Gegenstand	Action plan validated - [Current Action plan Name]
Inhalt	Dear Sir/Madam, The action plan [Action Plan Name] has been validated Thank you for your collaboration. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.

Begonnener Aktionsplan

Von	Freigabeverantwortlicher
An	Rechenschaftspflichtiger
Gegenstand	Action plan started - [Current Action plan Name]
Inhalt	Dear Sir/Madam, The following action plan has been assigned to you: "[Action Plan Name]". To enter the application and perform your task, [Click here]. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.

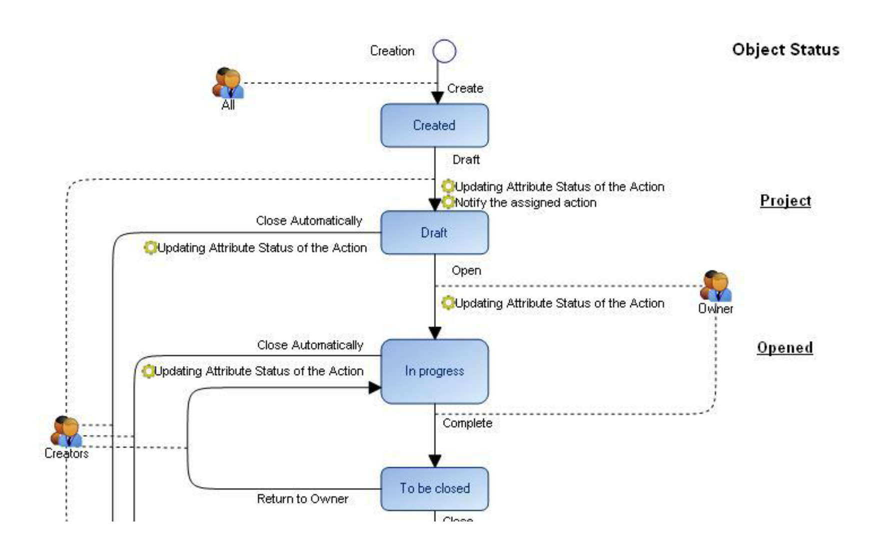
Zu schließender Aktionsplan

Von	Rechenschaftspflichtiger
An	Freigabeverantwortlicher
Gegenstand	Action plan to be closed- [Current Action plan Name]
Inhalt	The following action plan has been submitted for closure: "[Action Plan Name]". To enter the application and perform your task, [Click here]. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.

Geschlossener Aktionsplan

Von	Freigabeverantwortlicher
An	Rechenschaftspflichtiger
Gegenstand	Action plan closed - [Current Action plan Name]
Inhalt	Dear Sir/Madam, The action plan [Action Plan Name] has been closed. Thank you for your collaboration. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.

Schritte im Workflow einer Aktion



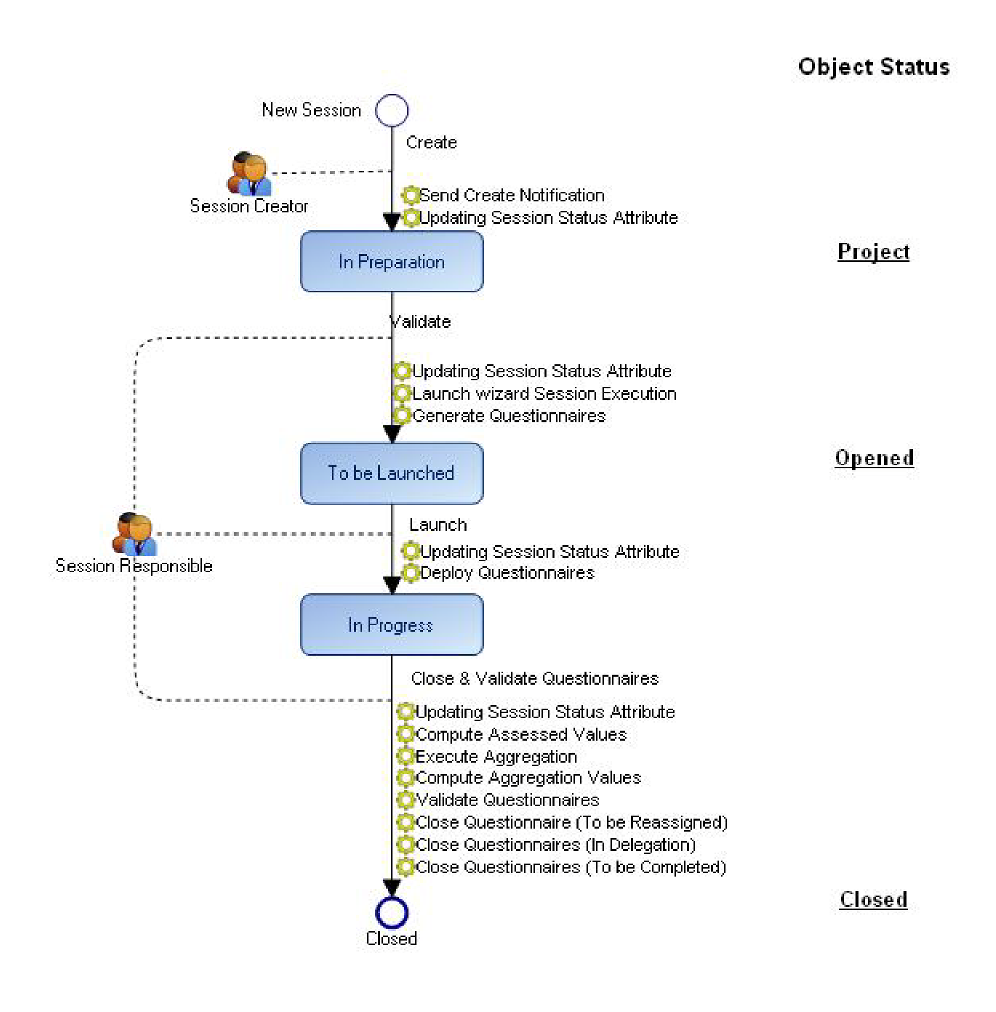
Benachrichtigungen im Workflow einer Aktion

Für Aktionen werden keine E-Mails vorgesehen. Vom Ersteller werden nur Benachrichtigungen an den Rechenschaftspflichtigen gesendet:

- wenn die Aktion einem Benutzer zugewiesen wird
- wenn die Aktion geschlossen wird

WORKFLOW EINER BEWERTUNGSSITZUNG

Die Schritte im Workflow einer Sitzung

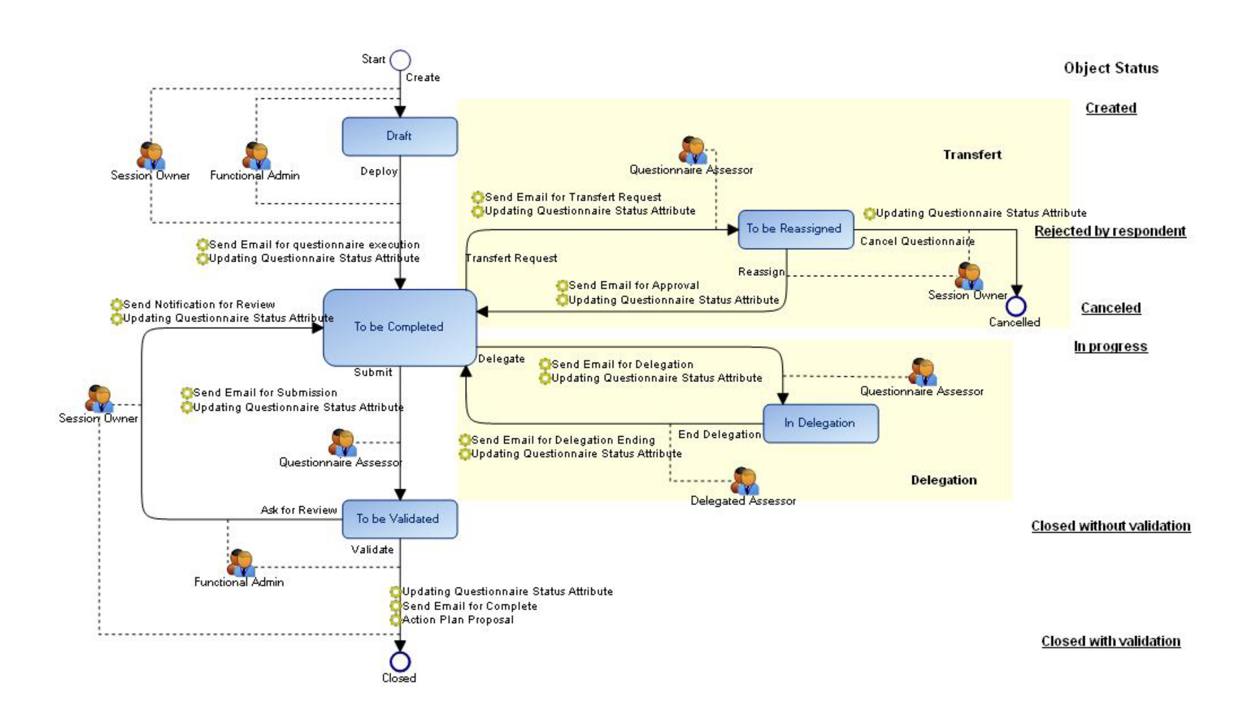


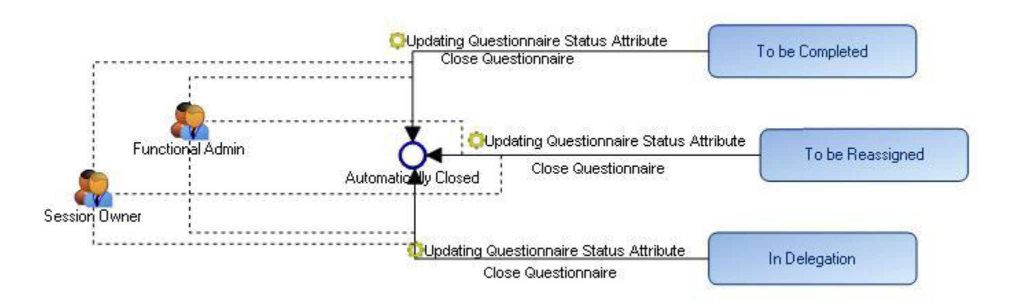
Die Benachrichtigungen im Workflow einer Sitzung

Für eine Sitzung werden keine E-Mails gesendet. Vom Ersteller wird nur eine Benachrichtigung an den Rechenschaftspflichtigen gesendet, der für die Sitzung bestimmt wurde.

Workflow eines Fragebogen

Die Schritte im Workflow eines Fragebogens





Die E-Mails im Workflow eines Fragebogens

Auszufülllender Fragebogen

Von	Ersteller
An	Für einen Fragebogen konsultiert
Gegenstand	Questionnaire to be completed - [Parent Session Name]
Inhalt	Dear Sir/Madam, A questionnaire has been sent to you by the risk management depertment. To enter the application and complete your questionnaire, [Click here]. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.

Neu zuzuweisender Fragebogen

Von	Für einen Fragebogen konsultiert
An	Rechenschaftspflichtiger einer Sitzung
Gegenstand	Questionnaire to be reassigned - [Parent Session Name]
Inhalt	[Respondent’s Name] has been requested that his/her questionnaire be reassigned. To enter the application and perform your task, [Click here]. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.

Demande de réassignation acceptée

Von	Rechenschaftspflichtiger einer Sitzung
An	Für einen Fragebogen konsultiert
Gegenstand	Questionnaire Transfer approved- [Parent Session Name]
Inhalt	Dear Sir/Madam, A questionnaire reassignment request has been approved. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.

Anforderung einer Delegation

Von	Beantworter
An	Delegierter Beantworter
Gegenstand	End of delegation - [Parent Session Name]
Inhalt	Dear Sir/Madam, A questionnaire from Risk Management has been delegated ti you by [Respondent’s Name]. To enter the application and perform your task, [Click here]. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.

Akzeptierte Anforderung einer Delegation

Von	Delegierter Beantworter
An	Beantworter
Gegenstand	End of delegation - [Parent Session Name]
Inhalt	Dear Sir/Madam, The questionnaire you have delegated to [Delegate Name] has been answered]. Please analyze the answers and send to the Risk Management department. To enter the application and perform your task, [Click here]. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.

Fragebogen einreichen

Von	Beantworter
An	Ersteller
Gegenstand	Questionnaire to be validated - [Parent Session Name]
Inhalt	Please validate the questionnaire submitted by [Respondent’s Name]. To enter the application and perform your task, [Click here]. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.

Freigegebener Fragebogen

Von	Ersteller
An	Beantworter
Gegenstand	Answers Approved - [Parent Session Name]
Inhalt	Dear Sir/Madam, Your answers to the questionnaire on [Parent Session Name] have been approved. Thank you for your collaboration. Comment: [Comment] This e-mail has been sent automatically by MEGA HOPEX.